Příloha č. 1

Technická specifikace

smlouvy o dodávce hardware a software a poskytnutí souvisejících služeb s názvem:

„Dodávka HW zařízení a SW aplikací – Městský úřad Jaroměř“

1. Předmět veřejné zakázky – technická specifikace HW zařízení a SW aplikací

1) Server vč. příslušenství

a) Host server – 2 ks

- Rackmount server o velikosti max. 2U včetně ramena pro vedení kabelů umožňujícího vysunutí zapnutého serveru z racku pro servisní účely.
- 1x procesor s možností osazení až 2 procesorů do serveru
- Výkon procesoru minimálně 513 bodů v benchmarku CPU2017 Integer Rates pro hodnoty ve sloupci Base Result. CPU musí podporovat rychlost přístupu k paměti minimálně v hodnotě 4800MT/s. Výsledek naměřených hodnot těchto CPU musí být pro daný chipset k ověření zveřejněný na stránkách www.spec.org
- RAM paměť o velikosti min. 384 GB typu DDR5 o rychlosti minimálně 4800MT/s, s možností budoucího rozšíření na min. 4096 GB a zároveň se zachováním instalovaných RAM modulů
- Bootovací zařízení osazené minimálně 2x 480GB NVMe diskem s hodnotou DWPD minimálně 3, hotplug provedení, RAID1
- Integrované diskové úložiště v provedení hotplug pro minimálně 8ks SFF 2,5“ disků s možností rozšíření až na 24ks SFF 2,5“ disků
- Minimálně 4 volné sloty standardu PCI-e 5.0
- 2x 10GbE SFP+ Ethernet port včetně transceiverů a optické kabeláže nebo jen DAC kabeláže na propojení s nabízenými LAN prvky v rámci racku. V případě varianty transceiverů, požadujeme doplnit originální transceivery do LAN switche. V případě DAC kabeláže požadujeme délku minimálně 3 metry, DAC kabely musí být originální a certifikované jak pro LAN switche tak i pro LAN kartu v serveru.
- 2x single portový SAN FC adaptér s rychlostí minimálně 32Gb
- 4x 1Gb LAN port 4x RJ-45 port
- 2x Napájecí zdroje s redundancí napájení 1+1, min. požadovaný výkon jednoho zdroje je minimálně 800W. Výkon zdrojů musí odpovídat doporučení výrobce pro danou konfiguraci serveru.
- Zdroje musí splňovat energetickou účinnost minimálně 96% (doložitelnou např. certifikací zdroje energetické účinnosti Titanium popř. čestným prohlášením výrobce)
- Management port RJ-45 pro vzdálenou správu serveru v plné konfiguraci. Pokud tato funkcionalita vyžaduje licenci, musí být licence součástí dodávky.
- Požadujeme vzdálený dohled výrobce serveru a automatické hlášení servisní události. Toto hlášení musí být zasláno automaticky a přímo servisnímu středisku.
- Management serveru musí být kompatibilní se stávajícími management nástroji zadavatele z důvod zachování ochrany investice.
- Management serveru musí být možné ovládat kdykoliv, z jakéhokoliv místa a zařízení pouze s připojením na internet.
- Server musí být schopen zajistit bezpečný provoz firmware komponent v serveru (minimálně HDD, SSD, síťové adaptéry, BIOS a vzdálenou správu) po celou dobu životnosti serveru. Server musí být schopen autonomně monitorovat autenticitu firmware na těchto komponentách. V případě zjištění neschváleného firmware musí být schopen automaticky uvést stav poškozené komponenty do bezpečného stavu. Pokud tato funkcionalita vyžaduje licenci, musí být součástí nabídky.
- Záruka min. 3 roky garantovaná výrobcem. Servisní zásah na místě u zákazníka musí být nejdéle následující pracovní den a tato služba musí být garantována výrobcem serveru. Délka záruky musí být ověřitelná na webu výrobce dle sériového čísla serveru.

- Zařízení musí být nové, nepoužité s garancí výrobce a určené přímo pro český trh.
- Pro centrální management požadujeme servery od totožného výrobce jako diskové pole, páskovou knihovnu a FC switche.

b) Management server – 1 ks

- Rackmount server o velikosti max. 2U včetně ramena pro vedení kabelů umožňujícího vysunutí zapnutého serveru z racku pro servisní účely.
- 1x procesor s možností osazení až 2 procesorů do serveru
- Výkon procesoru minimálně 280 bodů v benchmarku CPU2017 Integer Rates pro hodnoty ve sloupci Base Result. CPU musí podporovat rychlost přístupu k paměti minimálně v hodnotě 4800MT/s. Výsledek naměřených hodnot těchto CPU musí být pro daný chipset k ověření zveřejněný na stránkách www.spec.org
- RAM paměť o velikosti min. 128 GB typu DDR5 o rychlosti minimálně 4800MT/s, s možností budoucího rozšíření na min. 2048 GB a zároveň se zachováním instalovaných RAM modulů
- Bootovací zařízení osazené minimálně 2x 480GB NVMe diskem s hodnotou DWPD minimálně 3, hotplug provedení, RAID1
- Integrované diskové úložiště v provedení hotplug pro minimálně 8ks SFF 2,5“ disků s možností rozšíření až na 24ks SFF 2,5“ disků
- Minimálně 4 volné sloty standardu PCI-e 5.0
- 2x 10GbE SFP+ Ethernet port včetně transceiverů a optické kabeláže nebo jen DAC kabeláže na propojení s nabízenými LAN prvky v rámci racku. V případě varianty transceiverů, požadujeme doplnit originální transceivery do LAN switche. V případě DAC kabeláže požadujeme délku minimálně 3 metry, DAC kabely musí být originální a certifikované jak pro LAN switche tak i pro LAN kartu v serveru.
- 2x single portový SAN FC adaptér s rychlostí minimálně 32Gb
- 4x 1Gb LAN port 4x RJ-45 port
- 2x Napájecí zdroje s redundancí napájení 1+1, min. požadovaný výkon jednoho zdroje je minimálně 800W. Výkon zdrojů musí odpovídat doporučení výrobce pro danou konfiguraci serveru.
- Zdroje musí splňovat energetickou účinnost minimálně 96% (doložitelnou např. certifikací zdroje energetické účinnosti Titanium popř. čestným prohlášením výrobce)
- Management port RJ-45 pro vzdálenou správu serveru v plné konfiguraci. Pokud tato funkcionalita vyžaduje licenci, musí být licence součástí dodávky.
- Požadujeme vzdálený dohled výrobce serveru a automatické hlášení servisní události. Toto hlášení musí být zasláno automaticky a přímo servisnímu středisku.
- Management serveru musí být kompatibilní se stávajícími management nástroji zadavatele z důvod zachování ochrany investice.
- Management serveru musí být možné ovládat kdykoliv, z jakéhokoliv místa a zařízení pouze s připojením na internet.
- Server musí být schopen zajistit bezpečný provoz firmware komponent v serveru (minimálně HDD, SSD, síťové adaptéry, BIOS a vzdálenou správu) po celou dobu životnosti serveru. Server musí být schopen autonomně monitorovat autenticitu firmware na těchto komponentách. V případě zjištění neschváleného firmware musí být schopen automaticky uvést stav poškozené komponenty do bezpečného stavu. Pokud tato funkcionalita vyžaduje licenci, musí být součástí nabídky.

- Záruka min. 3 roky garantovaná výrobcem. Servisní zásah na místě u zákazníka musí být nejdéle následující pracovní den a tato služba musí být garantována výrobcem serveru. Délka záruky musí být ověřitelná na webu výrobce dle sériového čísla serveru.
- Zařízení musí být nové, nepoužité s garancí výrobce a určené přímo pro český trh.
- Pro centrální management požadujeme servery od totožného výrobce jako diskové pole, páskovou knihovnu a FC switche.

c) Záložní zdroj (typ I.) – 1 ks

- Výstupní výkon minimálně 6kW/6kVA
- Výstupy minimálně:
  - 1x Hard wire 3-wire (H N + E) (Battery Backup)
  - 2x IEC Jumpers (Battery Backup)
  - 4x IEC 320 C19 (Battery Backup)
  - 1x Hard Wire 3-wire (H N + G) (Battery Backup)
  - 6x IEC 320 C13 (Battery Backup)
- Vstupní napětí 230V 50/60Hz +/- 3%
- Výstupní napětí 230V
- Vstupní konektor: Hard wire 3-wire (1P + N + E)
- Technologie online s dvojitou konverzí
- Bypass součástí
- Porty: 1x RJ-45 10/100 Base-T, 1x RJ-45 seriál port, Smart slot, USB
- Výška maximálně 4U, provedení do racku
- Včetně komunikační karty a plné licence pro management UPS
- Multifunkční LCD displej a kontrolní konzolí
- Min. 3 roky záruka, včetně záruky na baterii

d) Záložní zdroj (typ II.) – 1 ks

- Výstupní výkon minimálně 2,7kW/3kVA
- Výstupy minimálně:
  - 3x IEC Jumpers (Battery Backup)
  - 1x IEC 320 C19 (Battery Backup)
  - 8x IEC 320 C13 (Battery Backup)
- Vstupní napětí 230V 50/60Hz +/- 3%
- Výstupní napětí 230V
- Vstupní konektor: Hard wire 3-wire (1P + N + E)
- Technologie line interactive
- Porty: 1x RJ-45 10/100 Base-T, 1x RJ-45 seriál port, Smart slot, USB
- Výška maximálně 2U, provedení do racku
- Včetně komunikační karty a plné licence pro management UPS
- Multifunkční LCD displej a kontrolní konzolí
- Min. 3 roky záruka, včetně záruky na baterii

2) Zálohovací pásková knihovna – 1 ks

- Knihovna musí obsahovat minimálně 24 slotů
- 2x FC drive minimálně LTO-8
- Instalace do racku, velikost max 2U

- Planá kapacita knihovny 288TB bez komprese, 720TB s kompresí
- Možnost mixovat LTO mechaniky různých generací
- Možnost mixovat LTO pásky různých generací
- 22ks minimálně LTO-8 RW medií včetně čárových kódů
- 1ks čistící LTO pásky
- Záruka min. 3 roky garantovaná výrobcem. Servisní zásah na místě u zákazníka musí být nejdéle následující pracovní den a tato služba musí být garantována výrobcem knihovny. Délka záruky musí být ověřitelná na webu výrobce dle sériového čísla knihovny.
- Zařízení musí být nové, nepoužité s garancí výrobce a určené přímo pro český trh.
- Pro centrální management požadujeme zálohovací páskovou knihovnu od totožného výrobce jako diskové pole, servery a FC switche.
- Součástí dodávky musí být kompletní instalace knihovny, včetně konfigurace a nastavení zálohovacích úloh dle požadavků zadavatele.

3) Firewall - 2 ks

- Firewall (bezpečnostní brána) včetně základních UTP služeb - 2 ks – zapojení ve vysoké dostupnosti
- Oba boxy v aktivním režimu
- Oba boxy s aktivní UTP licencí
- Porty minimálně:
  - 18x 1Gb RJ45 port
  - 2x 10Gb SFP+ porty
  - 4x 1Gb SFP port
  - 4x 1Gb combo port RJ45/SFP
  - 1x USB port
  - 1x console port
- Minimální propustnost firewallu IPv4 20 Gbps
- Minimální IPS propustnost min. 2.5 Gbps
- Minimální NGFW propustnost min. 1.5 Gbps
- Minimálně 1.5 miliony současných spojení
- Minimálně 55 tisíc nových spojení za sekundu
- Možnost vysoce dostupného zapojení dvou firewallů v režimu active-active
- Podpora LACP protokolu
- Podpora WAN load balancingu mezi primární a záložní linkou
- Funkce Load Balancing - možnost rozdělování zátěže
- Integrovaný bezdrátový kontroler umožňující plnou správu připojených SSID, podpora vytváření inteligentní bezdrátové sítě
- Podpora SSL Offloading
- Integrace do sandboxingu
- Podpora trafic shapingu pomoci definice aplikace nebo webové kategorie
- Podpora IPV6 - NAT46, 66, 64
- Funkcionalita Web filter - kontrola http a https provozu, kategorizace a selekce obsahu dostupného pro vybrané skupiny uživatel, blokování nežádoucích kategorií obsahu, antivirová kontrola stahovaného obsahu
- Integrovaná centrální správa endpoint security klientů z GUI firewallu s možností rozšíření počtu spravovaných klientů, možnost rozšíření o antivirovou funkčnost
- Včetně 10 virtuálních firewallů se samostatným administrativním rozhraním

- Možnost integrace 2faktorové autentizace klientů VPN či administrátorů firewallu bez nutnosti koupě a/nebo instalace dalšího backend či management software
- U software a firmware je vyžadována dostupnost bezpečnostních aktualizací po celou dobu udržitelnosti projektu (5 let)
- Základní UTP služby firewallu minimálně na 3 roky budou zahrnuty v ceně

4) Diskové pole – 2 ks

- Konfigurace s 16x 3,84TB pevný disk NVMe SFF SSD
- Kategorie diskového pole výrobcem určená pro podniky. Požadována je All NVMe architektura s garancí 100% dostupnosti dat.
- Záruka 100% dostupnosti dat musí být u nabízeného modelu jasně uvedena na webových stránkách dodavatele. Pokud výrobce přímo výslovně nepodporuje 100% dostupnost dat, pak musí nabídka obsahovat navíc další řadič a 10 % další kapacity jako rezervu (tzv. cold spare) pro zmírnění výpadků.
- Podpora obvyklé platformy operačních systémů a cluster funkcí včetně Windows Server 2019/2022, VMware ESXI 7/8, Red Hat Enterprise Linux (RHEL) a SUSE Enterprise Server (SLES) atd.
- Podpora front-end připojení protokolem NVMe over Fabrics (NVMe-oF) pomocí standardních fibre channel switchů o rychlosti 32 Gb/s.
- Nabízené úložiště musí být vybaveno alespoň dvěma řadiči.
- Užitná kapacita minimálně 30TB bez započtení redukčních mechanismů s použitím 3,84TB šifrovaných disků a musí být konfigurováno alespoň ochranou RAID 6. Dodavatel nesmí při návrhu pole použít u disků větší poměr datové a paritní kapacity než 10D+2P.
- Výkon alespoň 60.000 IOPS (kombinace čtení/zápis 70/30, 16kb datové bloky)
- Odolnost proti výpadku nejméně 2 disků současně v rámci jedné RAID skupiny.
- Výrobce musí nabízet pouze šifrované disky s příslušnými šifrovacími licencemi. Nepřipouští se žádné šifrování založené na řadiči nebo softwaru.
- Nabízené úložiště musí být skutečně aktivní, takže každý logický disk je rozdělen na všechny nabízené disky a všechny disky musí být schopny přispívat IO do obou řadičů současně.
- Požadované redundantní komponenty (tzv. No Single Point of Configuration): řadiče pole, cache, ventilátory, zdroje napájení.
- Paměť minimálně 512GB na obou řadičích.
- Nabízený řadič úložiště musí být založen na technologii alespoň PCIe 4.0 a nabízené úložiště musí mít alespoň 16 CPU jader.
- Minimálně 8 portů Fiber Channel 32 Gb/s osazené minimálně 4ks FC SFP transcieverů s možností rozšíření na 64 Gb/s pouze výměnou SFP transcieverů.
- Nabízené úložiště musí podporovat jak protokol Fiber Channel (FCP), tak NVMeOF over Fiber channel.
- Podpora osazení 2x 10/25Gb/s ethernetovými porty pro replikaci vlastními prostředky úložiště.
- Nativní podpora virtualizace, aby bylo možné vyčlenit svazky z logického prostoru namísto vyhrazení samostatných fyzických disků pro každou aplikaci.
- Úložiště musí mít distribuovaný globální rezervní prostor (global spare).
- Podpora inline engine s redukčními technologiemi pro efektivní ukládání dat (podpora Thin Zero detect and re-claim, De-duplication a Compression) a musí být ve výchozím nastavení povoleno. Dodavatel musí mít možnost flexibilně povolit / zakázat engine pro efektivitu dat v době vytváření svazku.

- Požadované funkce Thin Provisioning, Thin Re-claim, Snapshot, deduplikace, komprese, vzdálené replikace, monitoringu výkonu a kvality služeb pro dodanou kapacitu pole.
- Podpora nativní cloud konzoli pro správu neomezeného počtu polí.
- Aplikace pro správu musí být skutečně nativně cloudová, takže během životního cyklu smlouvy o podpoře musí být nabízena jako služba a není třeba aplikaci pro správu konfigurovat, aktualizovat, záplatovat.
- Monitoring s podporou cloudu, AI a analytický engine pro proaktivní správu úložiště a zmírnění rizik. Veškeré pro to požadované licence musí být součástí nabídky.
- Podpora kvality služeb pro kritické aplikace, aby bylo možné definovat vhodnou a požadovanou dobu odezvy pro logické jednotky aplikací v úložišti. Musí být možné definovat různé služby / doby odezvy pro různé aplikační logické jednotky.
- Řadiče úložiště musí mít podporu pro snapshoty (nejméně 1024 kopií pro daný svazek).
- Podpora nerušivé online aktualizaci firmwaru řadičů i diskových jednotek bez nutnosti restartu řadiče.
- Podpora hardwarové replikace dat na úrovni řadiče pole.
- Podpora skutečné active-active replikaci a funkci stretch clusteru pro nulové RPO a RTO tak, aby daný pár svazků mezi primární a DR lokalitou mohl mít souběžný přístup k operacím čtení i zápisu současně.
- Replikace typu active-active musí být podporována pro běžné operační systémy, jako je VMware, Redhat, Windows atd.
- Požadujeme technickou podporu výrobce po dobu 60 měsíců od převzetí zboží v režimu 24x7 se zahájením opravy v místě instalace nejpozději do 4 hodin po nahlášení závady. Požadujeme telefonickou podporu v režimu 24x7 se zpětným zavoláním nejpozději do 15 minut pro incidenty kritické závažnosti a do 1 hodiny pro ostatní incidenty.
- Obě disková pole musí obsahovat plné a neomezené licence pro active-active replikaci a tato replikace musí být dodavatele nakonfigurována a spuštěna
- Požadujeme certifikovanou instalace a konfiguraci výrobce zařízení.
- Požadujeme kompletní migraci dat ze současného diskového úložiště až do stavu, kdy bude moci být původní diskové pole odstaveno z provozu, bez jakýchkoli omezení provozu zadavetele.
- 8x kabel Flex LC/LC Multi-mode OM4 2 Fiber 5m
- Záruka min. 3 roky garantovaná výrobcem. Servisní zásah na místě u zákazníka musí být nejdéle následující pracovní den a tato služba musí být garantována výrobcem serveru. Délka záruky musí být ověřitelná na webu výrobce dle sériového čísla serveru.
- Zařízení musí být nové, nepoužité s garancí výrobce a určené přímo pro český trh.
- Pro centrální management požadujeme diskové pole od totožného výrobce jako servery, páskovou knihovnu a FC switche.

5) FC infrastruktura

a) FC Switch 32Gbit – 2 ks

- FC switch 24x 32Gb FC SFP28 port, rack provedení, výška 1U
- Každý switch včetně licence na minimálně 16ks FC 32Gb portů
- Všech 16ks FC 32Gb portů musí být osazeno příslušným 32Gb GBIC originálním modulem – přímo od výrobce FC switche
- 2ks 16Gb GBIC SFP+ LongWave 10km transceiver originální od výrobce switche
- Každý switch včetně 8ks LC/LC FC OM4 kabelů v délce 5m
- Agregovaná propustnost minimálně 768Gbps full duplex

- Doživotní záruka garantovaná výrobcem. Servisní zásah na místě u zákazníka musí být nejdéle následující pracovní den a tato služba musí být garantována výrobcem switche. Délka záruky musí být ověřitelná na webu výrobce dle sériového čísla switche.
- Zařízení musí být nové, nepoužité s garancí výrobce a určené přímo pro český trh.
- Pro centrální management požadujeme FC switche od totožného výrobce jako diskové pole, servery a páskovou zálohovací knihovnu.
- Součástí dodávky musí být kompletní instalace FC switchů, včetně konfigurace a nastavení zón dle požadavků zadavatele.

6) Switche - síťové přepínače LAN

a) LAN switch – 2 ks

- Modulární provedení switche, výška 1U, rozměr do racku 19‘
- 20x 10/100/1000BaseT port RJ-45
- Podpora plného managementu switche
- 4x Combo port 10/100/1000BaseT RJ-45 nebo 100M/1G SFP Port
- Technologie switche L3
- 1x uplink modulární slot s osazeným modulem 4x 10GbE SFP+ portem
- 1x stakovací modulární slot osazený 2 portovým stakovacím portem
- 1x stakovací kabel 0,5m
- 1x Dual Personality (RJ-45 or USB Micro-B) serial console port
- 1x USB A port pro uploading/downloading souborů
- 1x 100BASE-T Out of Band Management Port
- Propustnost minimálně 95 Mpps
- Stakovací výkon minimálně 100 Gbps
- Switchovací kapacita minimálně 128 Gbps
- Velikost routovací tabulky minimálně 2.000 IP adres IPv4, 1.000 IP adres IPv6, 200 QSFP, 256 statických
- Velikost tabulky Mac adres minimálně 32.000 záznamů
- Součástí každého switche musí být 2x 10GbE SFP+ transceiver LC LR 10km
- Podpora protokolu IEEE 802.3bz
- Switch osazený dvojicí redundantních napájecích zdrojů s možností výměny za chodu, minimální výkon 250W
- Každý switch osazený 2x 10Gb SFP+ LC LR 10km transceiverem, originální, od výrobce switche
- Doživotní záruka garantovaná výrobcem. Servisní zásah na místě u zákazníka musí být nejdéle následující pracovní den a tato služba musí být garantována výrobcem switche. Délka záruky musí být ověřitelná na webu výrobce dle sériového čísla switche.
- Zařízení musí být nové, nepoužité s garancí výrobce a určené přímo pro český trh.
- Pro centrální management požadujeme LAN switche od totožného výrobce jako diskové pole, servery a páskovou zálohovací knihovnu.
- Součástí dodávky musí být kompletní instalace LAN switchů, včetně konfigurace a nastavení zón dle požadavků zadavatele.

7) WiFi - bezdrátové prvky

Bezdrátové prvky wifi - dodávka musí obsahovat veškeré potřebné licence pro využití všech funkcí nabízeného zařízení. Dostupnost aktualizací a podpory po celou dobu udržitelnosti projektu (5 let).

a) Přístupový bod / Access Point (AP) – 20 ks

Minimální požadavky:

- Uzavřená konstrukce bez ventilátorů
- Podpora bezdrátových standardů: 802.11a/b/g/n, 802.11ac wave2, 802.11ax
- Plnohodnotná certifikace Wi-Fi Aliance: IEEE 802.11a/b/g/n/ac
- Plnohodnotná certifikace Wi-Fi Aliance: WPA3-CNSA, WPA3-SAE, WPA3-OWE
- Pracovní režim AP bez kontroléru (autonomní)
- Pracovní režim AP řízené kontrolérem (lightweight)
- Pracovní režim AP v roli kontroléru s možností správy až 120 AP
- Minimální počet portů ethernet LAN: 2x 100/1000 Mbit/s RJ45
- Podpora muligigabit ethernet 2.5 Gbps IEEE 802.3bz
- Podpora standardů IEEE 802.3af (PoE), IEEE 802.3at (PoE+) a IEEE 802.3bt
- Podpora linkové agregace LACP
- Podpora standardního PoE+ IEEE 802.3at 30W bez nutnosti redukce výkonu libovolného rádia
- Podpora napájení z AC napájecího zdroje
- Vestavěná interní anténa MIMO, omni down-tilt
- Radiová část: dual band, současná podpora pásem 2,4GHz a 5GHz
- MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2 a MIMO a počet nezávislých streamů na 5GHz rádio: 4x4:4
- Podpora šířky kanálu 160 MHz
- HW podpora DL-OFDMA, UL-OFDMA a DL-MU-MIMO
- Automatické ladění kanálu a síly signálu v koordinaci s ostatními AP
- Možnost nastavení vysílacího výkonu s krokem 0.5 dBm
- Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 5GHz: 4800 Mbps a pro 2.4GHz: 575 Mbps
- Integrovaný TPM pro bezpečné uložení certifikátů a klíčů
- Podpora 802.11ac explicitního beamformingu
- Podpora airtime fairness
- Prioritizace jednotlivých SSID na základě vysílacího času
- USB port s podporou 3G/4G USB modemu jako WAN uplink
- Vypínatelné indikační LED diody informující o stavu zařízení
- Band Steering či obdobné (prioritizace 5GHz pásma v případě je-li podporováno)
- Detekce Rogue AP
- Minimální počet inzerovaných SSID (BSSID) na radio: 16
- Nastavitelný DTIM interval pro jednotlivé SSID
- Mapování SSID do různých VLAN podle IEEE 802.1Q
- VLAN Pooling
- HW Podpora wireless MESH funkcionality s protokolem pro optimální výběr cesty v rámci MESH stromu
- Podpora Layer-2 izolace bezdrátových klientů
- HW Podpora spektrální analýzy v pásmech 2,4GHz a 5GHz
- Hardware filtry pro filtraci intermodulačního rušením pocházejícím z mobilních sítí (Advanced Cellular Coexistence nebo obdobné)

- Detekce a monitorování problémů WLAN odchytáváním provozu na AP ve formátu PCAP a jeho zasíláním do Ethernetového analyzátoru, schopnost zachytávat rámce včetně 802.11 hlaviček
- DHCP server, směrování a NAT pro bezdrátové klienty
- AP v režimu IPSec VPN klient s možností tvorby L2 či L3 VPN
- Automatická identifikace připojeného zařízení a jeho operačního systému
- Předávání konektivity mezi AP při pohybu bez výpadku spojení – roaming
- Dynamické vyvažování zátěže klientů mezi AP se zohledněním zátěže, počtu klientů, síly signálu v koordinaci s ostatními AP
- Optimalizace provozu: multicast-to-unicast konverze
- Možnost řízení QoS (šířky pásma) na základě aplikací (Office 365, Dropbox, Facebook, P2P sdílení, VoIP, video aplikace)
- Filtrování přístupu na web
- Podpora RadSec (RADIUS over TLS)
- 802.11w ochrana management rámců
- Podpora Kensington lock
- Podpora MAC ověřování a 802.1X ověřování s využitím lokální DB v AP
- Podpora 802.1X suplicant, AP se ověřuje před připojením do LAN
- CLI formou serial konsole port a serial over Bluetooth
- SSHv2, SNMPv2c a SNMPv3
- AP podporuje zero touch provisioning pomocí externího management SW, jehož IP adresu získá z cloud aktivační služby poskytované výrobcem
- Integrované Bluetooth 5.0 Low Energy (BLE) rádio
- Integrované Zigbee 802.15.4 rádio
- Podpora režimu SLEEP s max. spotřebou energie do 6W
- Záruka min. 3 roky

Součástí každého dodávaného AP bude příslušenství pro montáž na zeď nebo strop.

8) NAC - Network Access Control – 1 ks

- Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN připojení
- Forma dodání: virtuální appliance pro VMware
- Minimální celková kapacita řešení pro autentizaci unikátních 100 koncových zařízení
- Možnost vytváření clusteru více virtuálních appliance. Minimální počet podporovaných appliance v clusteru
- Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance
- Podpora minimálně 20ti předních světových výrobců síťových zařízení (LAN switche, WiFi řešení, obecně přístupové datové sítě)
- Požadované metody autentizace uživatelů a zařízení:PEAP-MSCHAPv2, EAP-TLS, EAP-TTLS, MAC autentizace
- Podpora RADIUS CoA dle RFC3576
- Podpora autorizace zařízení a uživatelů na základě kontextových informací jako čas, místo připojení, osobní profil či skupina v AD

- Možnost autorizace uživatelů na základě jejich vlastních accounting informací z předchozích připojení – např. za účelem omezení celkového času online či objemu přenesených dat za delší časové období
- Možnost TACACS+ autentizace správců síťových zařízení
- Další požadované autentizační a autorizační zdroje a metody: LDAP, MS AD, Token, MAC, generická SQL databáze, Kerberos, HTTPS web autentizace, Single Sign-On (minimálně SAML 2+ IdP a SP, OAuth, Shibboleth a Okta)
- Možnost integrace s MDM (Mobile Device Management) platformami třetích stran: minimálně AirWatch, Citrix, MobileIron, JAMF, InTune
- Podpora REST API pro většinu základních úkonů AAA platformy
- Podpora REST volání vyvolaného autentizační či autorizační událostí (minimálně pro předání informací o klientovi jinému systému, automatického založení support ticketu atp.)
- Zpracovávání syslog hlášení z externích zdrojů, vyhledávání klíčových událostí a automatizovaná reakce na ně. Minimálně v rozsahu přijmutí bezpečnostního hlášení z firewallu a izolace konkrétního klienta na základě tohoto hlášení.
- Administrátor systému musí mít možnost vlastní tvorby parseru/integrace syslog hlášení pro možnost uživatelské integrace s libovolnými systémy třetích stran.
- Sběr dodatečných informací o připojených zařízeních (“profiling”) jako jsou DHCP volby klienta, HTTP uživatelský agent či předvolba MAC adresy. Tyto informace musí být možné využít pro doplňkové ověření přístupu zařízení do sítě.
- LAN a WLAN Guest portál. Portál musí podporovat možnost přihlašování přes účty minimálně těchto sociálních sítí – Linkedln, Facebook, Twitter, Google+. Portál musí umožňovat bohatou grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě s SMS, email ověřením nebo na elektronickou notifikaci a schválení pověřených pracovníků.
- Možnost licenčního rozšíření o bezpečnou registraci soukromých zařízení do interní sítě na základě uživatelských údajů z AD či LDAP. Uživatel musí být schopen jednoduchým uživatelským wizardem instalovat osobní certifikát a síťový profil na své soukromé zařízení (BYOD systém).
- Možnost licenčního rozšíření o certifikační autoritu pro vydávání certifikátů na soukromá zařízení musí být součástí AAA platformy.
- Možnost licenčního rozšíření o samoobslužný portál pro hosty či interní uživatele s možností správy svých vlastních registrací.
- Možnost licenčního rozšíření o systém pro bezpečnostní kontrolu přistupujících zařízení před jejich vpuštěním do sítě pomocí software agenta na koncová zařízení.
- Možnost licenčního rozšíření o kontroly stavu registrů, spuštěných procesů, stavu síťových zařízení, nastavení firewallu, aktualizace antivirů, instalované VM, stav enkrypce disku.
- Možnost licenčního rozšíření o podporu jednorázového i permanentního klienta pro kontroly na koncových zařízeních. Podpora klienta pro kontrolu koncových zařízení na OS Windows, MAC OS a Linux
- Možnost licenčního rozšíření o integraci tohoto koncového klienta s VPN klientem

- Jakékoliv funkční rozšíření systému musí být vždy v rámci stejné virtuální appliance jako je AAA systém.
- Servisní podpora na 3 roky garantovaná přímo výrobcem zařízení v režimu 24x7. Možnost otevírat servisní požadavky přímo u výrobce.

9) Sada licencí software – suma

- Požadujeme v nabídce, ve smlouvě a faktuře přesnou identifikaci zařízení produktovým číslem výrobce (tzv. Part Number), v případě dodání licence operačního systému jinou formou než prostřednictvím výrobce (OEM), požadujeme identifikaci licence operačního systému pomocí Part Numberu výrobce s plným názvem licence. Zadavatel si vyhrazuje právo ověřit si konfiguraci SW daného produktu u výrobce nebo autorizovaného distributora, jestli odpovídá údajům uvedeným v nabídce, smlouvě a faktuře.
- 2x operační serverový systém v nejnovější verzi, plně kompatibilní se současnými serverovými operačními systémy zadavatele. Licence na minimálně 16 procesorových jader. Licence bez omezení počtu provozovaných virtuálních serverů.
- 2x operační serverový systém v nejnovější verzi, plně kompatibilní se současnými serverovými operačními systémy zadavatele. Licence na minimálně 16 procesorových jader. Licence pro 2ks provozovaných virtuálních serverů.
- 10x instalace operačního serverového systému ve virtualizované verzi
- 10x migrace operačního serverového systému z provozované verze na nově dodávanou
- 150x klientská licence pro serverový operační systém v nejnovější verzi a plně kompatibilní se současnými i nově dodávanými serverovými operačními systémy zadavatele
- 1x komunikační serverový systém v nejnovější verzi, plně kompatibilní se současnými komunikačními serverovými systémy zadavatele. Licence na minimálně 16 procesorových jader. Musí se jednat o systém, který umožní plnou a bezzásahovou migraci serveru, účtů, poštovních schránek, archivů, .pst souborů ze současného komunikačního serveru zadavatele.
- 150x klientská licence pro komunikační serverový systém v nejnovější verzi a plně kompatibilní se současnými i nově dodávanými serverovými komunikačními systémy zadavatele
- Součástí dodávky musí být migrace komunikačního serverového systému ze současného na nově dodávaný
- 2x databázový serverový systém v nejnovější verzi, plně kompatibilní se současnými serverovými databázovými systémy zadavatele. Licence pro neomezený počet uživatelů. Licence s předplatnými na minimálně 3 roky.
- 2x Instalace databázového serverového systému s migrací databází z provozovaných databázových serverů

10) Zálohovací systém – 4 ks

- Licence pro zálohování 20ks virtuálních serverů
- Zálohovací řešení musí podporovat infrastrukturu VMware ve verzích 6.x, 7.x a 8.0, včetně VMware Cloud Foundation, VMware Cloud on AWS, VMware cloud on Dell a Azure VMware Solution
- Řešení musí podporovat hostitele spravované serverem VMware vCenter ve verzích 6.x, 7.x a 8.0 i samostatné ESXi hostitele.

- Zálohovací řešení musí podporovat Windows Server Hyper-V 2012 až 2022 včetně Server Core, Azure Stack HCI i Microsoft Hyper-V Server
- Řešení musí podporovat hostitele spravované pomocí Microsoft System Center Virtual Machine Manager 2012 R2 až 2019, klastrové i samostatné hostitele Hyper-V
- Řešení musí podporovat zálohování všech operačních systémů, které jsou podporovány pro provoz na těchto hypervizorech
- Řešení musí podporovat zálohování platformy Red Hat Virtualization 4.4 SP1
- Řešení musí podporovat zálohování celých zařízení NAS, jednotlivých sdílených složek SMB a NFS a souborových serverů Windows a Linux.
- Software musí být možné licencovat pomocí trvalé licence i formou časově omezené subscripce.
- Řešení nesmí být závislé na jednom poskytovateli HW, virtualizační, nebo cloudové platformy, a to jak pro výpočetní část, tak pro část ukládání dat.
- Licence musí být přenositelná mezi různými fyzickými, virtuálními a cloudovými chráněnými objekty
- Všechny součásti řešení musí plně podporovat komunikaci po IPv6
- 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.
- Řešení musí poskytovat jednotnou konzoli pro přehled o zálohách fyzických, virtuálních, cloudových, NAS i Kubernetes prostředí
- Řešení musí umožnit vytvoření jednoho logického úložiště pro ukládání záloh z neomezeného počtu různorodých diskových úložišť
- Řešení musí umožňovat ukládání záloh do různých diskových úložišť, souborových systémů, objektových úložišť, nebo deduplikačních diskových zařízení.
- Řešení musí využívat mechanismus sledování změn bloku. Pro všechny podporované hypervizory musí být implementace CBT certifikována výrobcem hypervizoru
- Výše uvedená funkce musí být konfigurovatelná na úrovni datastore virtualizační platformy
- Řešení musí umožňovat vytváření záloh integrací se snímky úložiště. Dále musí umožnit obnovu jednotlivých VM, souborů a položek aplikace z těchto snímků. Proces zálohy nemůže k připojení snímku použít dočasného hostitele. Popsaná funkce musí fungovat pro prostředí VMware vSphere a musí podporovat min. následující pole: Dell, NetApp, HPE, HITACHI VANTARA, IBM, Lenovo, Fujitsu, Pure Storage, CISCO, DataCore
- 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
- 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
- Uvedená funkce musí umožňovat spuštění zálohy vytvořené z různých platforem (různých virtuálních, fyzických a veřejných cloudových virtuálních strojů)
- 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.
- Řešení musí umožňovat prezentaci disků přímo ze záložního souboru do spuštěné VMware VM
- Přístup do řídící konzole musí být chráněný vícefaktorovou autentizací bez nutnosti přístupu k internetu.

- Řešení musí umožňovat vytváření záloh odolných vůči náhodnému, či úmyslnému smazání, nebo ransomware útokům na komoditním serverovém HW, nebo jakémkoliv S3-kompatibilním objektovém úložišti
- Řešení musí podporovat gMSA účty pro zajištění aplikačně-konzistentních záloh v GuestOS bez nutnosti ukládání přístupových oprávnění na úrovni administrátora pro daný GuestOS.
- 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
- Řešení musí umožňovat pravidelné automatické testování obnovitelnosti záloh, včetně funkčnosti jednotlivých služeb a kontrolou obsahu na kybernetické hrozby pomocí řešení třetích stran.
- Řešení musí poskytovat dohled nad chráněnou virtualizační platformou, poskytující včasná varování před výpadkem, nebo omezením dostupnosti produkčního prostředí
- Řešení musí poskytovat možnost dohledu služeb a procesů provozovaných v GuestOS jednotlivých chráněných VM
- Řešení musí informovat, které VM nejsou chráněné dostatečně, nebo vůbec a zároveň kdy a jakým způsobem byl naposledy vytvořen bod obnovy.
- Řešení musí poskytovat možnost automatizovaných řešení chybových stavů
- Řešení musí poskytovat funkce pro zasílání stavových hlášení do centrálního monitorovacího nástroje přes SNMP protokol
- Řešení musí podporovat monitorování virtualizovaných prostředí VMware vSphere a Microsoft Hyper-V bez nástrojů třetích stran
- Řešení musí podporovat dohled min. následujících systémů: VMware, ESXi 6.x, 7.x a 8.0 pro placené i bezplatné edice ESXi. Podporovaní hostitelé mohou být spravováni pomocí vCenter serveru nebo pracovat v samostatném režimu
- Řešení musí poskytovat historická data a predikce z nich vyplývající, nezbytné pro plánování zdrojů pro provoz a ochranu virtualizovaného prostředí
- Součástí řešení musí být i možnost vytvářet detailní auditové správy o změnách v konfiguraci zálohovacího řešení a o obnovách dat ze záloh
- Řešení musí podporovat reporting virtualizovaných prostředí VMware vSphere a Microsoft Hyper-V bez nástrojů třetích stran
- Řešení musí podporovat reporting min. následujících hypervisorových systémů: VMware, ESXi 6.x, 7.x a 8.0 pro placené i bezplatné edice ESXi. Podporovaní hostitelé mohou být spravováni vCenter nebo pracovat v samostatném režimu
- Řešení musí podporovat reporting min. následujících systémů: Microsoft Server Hyper-V 2012, 2012R2, 2016, 2019 a 2022 pro placené i bezplatné edice. Podporovaní hostitelé mohou být spravováni SCVMM nebo pracovat v samostatném režimu
- Řešení nesmí vyžadovat instalaci žádných agentů na monitorovaných hostitelích ESXi a Hyper-V a na virtuálních počítačích

11) Bezpečnostní software – 180 ks

Licence komplexního SW pro ochranu před škodlivým softwarem pro 180 uživatelů, včetně příslušenství uvedeného níže v podobě EDR a Sandboxu pro tyto licence.

Podpora operačních systémů MS:

- Windows 7 a vyšší
- Windows Server 2008 R2 a vyšší

Antivirový klient pro systémy:

- Windows
- Linux
- macOS
- Android

Real-Time ochrana před všemi typy PUA a malwaru:

- viry
- červy
- trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware…)

Správa zařízení pro Windows, macOS a Linux, umožňující blokaci externích zařízení a médií, s podporou whitelistování dle:

- výrobce, modelu nebo sériového čísla,
- uživatelů nebo skupin (např.administrátorů) v AD,
- lokálního času.

Schopnost blokace přístupu na definované weby nebo skupiny webů dle kategorií s možností whitelistování dle přihlášeného uživatele/skupiny v AD nebo času.

- Lokální anti-spam s úspěšností detekce 99 % a vyšší.
- Lokální anti-spam s možností definování důvěryhodných a spamových adres.
- Nativní 64 bitové jádro.
- Ochrana komunikace e-mailovými protokoly:
  - POP3,
  - POP3S,
  - IMAP,
  - IMAPS,
  - HTTP,
  - MAPI.
- Antivirus, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb.
- Personální firewall pro zabránění neautorizovanému přístupu k zařízení se schopností automatického přebrání pravidel z brány Windows Firewall.
- HIPS (Host-based Intrusion Prevention System) pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení.
- Aktivní i pasivní heuristická analýza pro detekci
- dosud neznámých hrozeb.
- Systém pro blokaci exploitů zneužívajících zeroday zranitelností, jenž pokrývá nejpoužívanější vektory útoku:
  - síťové protokoly,
  - Flash Player,
  - Javu,
  - Microsoft Office,
  - webové prohlížeče,
  - e-mailové klienty,
  - PDF čtečky…
- Systém pro detekci malwaru již na síťové úrovni poskytující ochranu i před zneužitím
- zranitelností na síťové vrstvě.
- Anti-phishing se schopností detekce homoglyph útoků.
- Kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování.

- Možnost jednotlivého zapnutí detekcí:
  - potenciálně nechtěných aplikací,
  - zneužitelných aplikací,
  - podezřelých aplikací.
- Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů.
- Kontrola souborů v průběhu stahování pro snížení celkového času kontroly.
- Detekce s využitím strojového učení.
- Funkce ochrany proti zapojení do botnetu pracující s detekcí síťových signatur.
- Ochrana před síťovými útoky skenující síťovou komunikaci a blokující pokusy o zneužití zranitelností na síťové úrovni.
- Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací.
- Lokální sandbox.
- Speciální modul behaviorální analýzy pro detekce nových typů ransomwaru.
- Systém reputace pro získání informací o závadnosti souborů a URL adres.
- Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur.
- Technologie pro detekci rootktitů obvykle se maskujících za součásti operačního systému.
- Skener firmwaru BIOSu a UEFI.
- Skenování souborů v cloudu OneDrive.
- Šetření baterie notebooku – možnost odložení kontroly / provádění aktualizací, pokud je zařízení napájeno z baterie.
- Podpora dotykového ovládání.
- Ovládání bezpečnostního programu pomocí Příkazového řádku.
- Podpora ochrany na IPv6.
- Možnost řízení šířky pásma pro stahování aktualizací.
- HIPS s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory.
- Možnost vrácení i odložení aktualizací signatur.
- Možnost instalovat plnohodnotné antivirové řešení na virtuální stanici/server.
- Modulární instalace.
- Automatická synchronizace bezpečnostních produktů v clusteru.
- Bez-agentové zabezpečení pro VMware vShield aNSX.
- Možnost importu/exportu nastavení.
- Prezentační režim umožňující potlačení méně důležitých upozornění při práci v celoobrazovkovém režimu aplikace.
- Možnost tvorby výjimek na procesy.
- Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení souborů operačního systému.
- Možnost vzdáleného definování akce připojení výměnných médií (kontrolovat, nekontrolovat, nechat na uživateli).
- Možnost využití sdílené cache v rámci lokální sítě (umožňuje přeskočení skenování stejných souborů, které již byly zkontrolované na jiném zařízeních a tím výrazně zrychlit kontrolu).
- Duální aktualizační profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (pro cestující uživatele s notebooky).
- Kontrola šifrovaných spojení (SSL, TLS, HTTPS,IMAPS…).
- Možnost odesílání e-mailových upozornění a událostí přímo z klienta.
- Integrovaný komplexní diagnostický nástroj umožňující řešit problémy s infiltrací, jakožto i jiné softwarové a hardwarové nekorektní chování (obsahuje informace procesech, službách, síťových připojeních, ovladačích a problémových položkách v registrech).

- Upozornění při připojení k nezabezpečené bezdrátové síti nebo síti se slabým zabezpečením, jejíž šifrování lze snadno prolomit.
- Využití Microsoft Antimalware Scan Interface (AMSI) pro kontrolu skriptů (PowerShell, wscript.exe a cscript.exe).
- Podpora Protected Services – službu produktu je možné chránit proti nechtěné modifikaci standardní součástí operačního systému.
- Podpora odečítače obrazovky pro zrakově postižené.
- Podpora SNMP Trap, Syslogu a qRadar SIEM.
- Podpora instalace skriptem - *.bat, *.sh, *.ini (GPO, SSCM…).
- Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu.
- Reportování stavu klientů chráněných jinými bezpečnostními programy.
- Schopnost zaslat reporty a upozornění na email.
- Přidání zařízení do vzdálené správy pomocí:
    - synchronizace s Active Directory,
    - ruční přidání pomocí dle IP adresy nebo názvu zařízení,
- pomocí síťového skenu nechráněných zařízení v síti.
- Je požadována dodávka licence s délkou trvání min. 3 let, včetně nároků na nové verze software po tuto dobu.

a) Odhalení škodlivé, či podezřelé aktivity tzv. EDR

- Podpora Windows a macOS.
- Indicators of Compromise (IOCs):
    - MD5 hodnoty souborů,
    - IP adresy a URL,
    - Nesoulad názvů souborů/procesů,
    - Neobvyklé využití aplikací a síťových portů,
    - Neobvyklé injektování do procesů,
    - Modifikace částí aplikací,
    - Změny v registru.
- Indikátory útoku pracující s behaviorální detekcí.
- Indikátory útoku pracující s reputací.
- Možnost tvorby vlastních IoC.
- Řešení umožnuje analýzu vektorů útoku.
- Vizibilita do WMI.
- Vizibilita do spouštěných skriptů (PowerShellem, CScriptem, WScriptem…).
- Přehled o veškerém použitém softwaru a jeho verzích.
- Schopnost detekce škodlivých spustitelných souborů a skriptů.
- Pokročilé možnosti analýzy:
    - exploitů,
    - rootkitů,
    - síťových útoků,
    - bezsouborového malwaru.
- Schopnost analýzy RAM paměti.
- Detekce rootkitů v UEFI a MFT.
- Schopno detekovat laterální pohyb útočníka.
- Tagování objektů.
- Terminal (interaktivní Shell).

- Možnost ruční analýzy procesů a veškerýchspustitelných souborů včetně DLL knihoven a skriptů.
- Prioritizace vzniklých incidentů za pomocí algoritmů strojového učení.
- Detekce více než 300 typů obecného podezřelého chování: dumpování přihlašovacích údajů, změna konfigurace firewallu, mazání logů, změna hosts souboru, smazání Shadow Copy, nainstalování nového certifikát, vypnutí aktualizací…
- Detekce s využitím modelů strojového učení a neuronových sítí.
- Schopnost zobrazení detekcí provedených antimalware produktem.
- Možnost spouštět předkonfigurované nápravné akce, které se sami spustí za při splnění definovaných podmínek.
    - Okamžitá síťová izolace, ukončení procesu, vymazání/stažení souboru.
- Snížení počtu falešně pozitivních výsledků za pomocí algoritmů strojového a hlubokého učení.
- Řešení je schopno generovat tzv. forest / full execution tree model.
- Možnost vyhledávání pomocí nově vytvořených IoC nad historickými daty.
- Provázání s technikami popsanými v knowledge base MITRE ATT&CK.
- Možnost analyzovat
    - veškeré události až 3 měsíce zpětně,
    - bezpečnostní incidenty až 3 roky zpětně.
- Možnost provozu v offline prostředí.
- Možnost logování činností uživatele.
- Přihlašování do konzole za využití 2FA.
- Podpora exportu do SIEMu.
- REST API.
- Možnost provozu EDR serveru na systému Windows.
- Možnost provozu centrálního serveru on-premise.
- Možnost provozu s databázemi:
- • MS SQL,
- • MySQL.

b) Sandboxing

- Sandbox umožňující spuštění vzorků malwaru pro:
    - Windows,
    - macOS,
    - Linux,
    - Android.
- Možnost využití na koncových bodech a Exchange serveru pro aktivní detekci škodlivých souborů v emailech.
- Řešení zajišťuje neodesílání duplicitních souborů nalezených různými endpointy.
- Analýza neznámých vzorků v řádu jednotek minut.
- Schopnost ochrany klientů mimo firemní síť.
- Optimalizace pro znemožnění obejití anti-sandbox mechanismy.
- Schopnost analýzy rootkitů a ransomwaru.
- Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti.
- Řešení pracuje s behaviorální analýzou.
- Manuální odeslání vzorku do sandboxu.
- Funkce cloudového sandboxu je integrována do antimalware produktu (cloudový sandbox nemá vlastního agenta).

- Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu.
- Neomezené množství odesílaných souborů.
- Veškerá komunikace probíhá šifrovaným kanálem.
- Webová konzole.
- Administrace v nejpoužívanějších jazycích včetně češtiny.
- Možnost nastavení typů odesílaných souborů:
  - spustitelné soubory,
  - skripty,
  - spam,
  - dokumenty.
- Přehled o veškerých odeslaných souborech ve správcovské konzoli.
- Nastavení per zařízení & per skupina.
- Možnost nastavit na výsledek sandboxu výjimku.
- Zaslání e-mailové notifikace v případě nalezení škodlivého kódu.
- Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
- Server/proxy architektura pro síťovou pružnost – snížení zátěže.

12) 2-faktorové ověřování – 100 ks

- OTP 2FA řešení kompatibilní s poptávaným firewallem ve formě mobilní aplikace pro 50 uživatelů
  - Šifrovací algoritmus OATH-TOTP (RFC6238, RFC 4226)
  - Podporované systémy: iOS (iPhone, iPod Touch, iPad, iWatch), Android, Windows Phone 8/8.1, Windows 10 and Windows Universal Platform
- 100ks OTP 2FA řešení kompatibilní s poptávaným firewallem ve formě HW tokenu
  - Šifrovací algoritmus OATH-TOTP (RFC6238)
  - 6-ti místný kontrastní LCD displej
  - Provedení IP54
  - OTP specifikace: 60 sec, SHA-1

13) NDR - Network Detection and Response – 1 ks

- Monitorovací systém pro dlouhodobé a detailní monitorování veškerého provozu v počítačové síti
- Systém musí umožňovat v reálním čase vyhodnocovat objemy a struktury provozu, analyzovat příčiny provozních či výkonnostních problémů a odhalovat bezpečnostní hrozby.
- Systém musí být nezávislý na použité síťové infrastruktuře
- Systém nesmí svou funkcí monitorovanou síť ovlivňovat
- Vyhrazená HW sonda pro monitoring datových toků v kombinaci s integrovaným kolektorem zajistí monitoring, sběr, uchování a reporting Flow dat. Sonda bude instalována na rozhraní WAN. V rámci dodávky bude nakonfigurováno min. 5 reportů a bude zaškolena lokální administrátor sítě v rozsahu min. 0,5 den. Součástí konfigurace bude nastavení servisních protokolů NTP, SSH, HTTPS, SNMP atd.
- Sonda má 1 x 10/100/1000 monitorovací port (UTP kabeláž)
- Pasivní zapojení bez vlivu na monitorovanou síť a propustnost zařízeni (zapojení pomocí TAP sdružujícího obousměrný monitorovaný tok do jedné linky).

- Jeden plnohodnotný management port 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu
- Zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS.
- Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí.
- Možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s na metalickém rozhraní.
- Podpora pro SNMP
- Vestavěný kolektor pro dočasné ukládání flow statistik (zajištění redundance), který zahrnuje plnohodnotnou funkcionalitu flow kolektoru a uložení dat po dobu min. 2 měsíců
- Úložná kapacita vestavěného kolektoru min. 0,5 TB
- Výkon vestavěného kolektoru min. 50 000 toků/s
- Časová synchronizace zařízení proti centrálnímu zdroji času na síti (NTP).
- Minimální výkon 1 milion paketů za sekundu na každém portu.
- Jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.
- Možnost přístupu a konfigurace hardwarových zařízení prostřednictvím sériové linky (RS-232).
- Použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.
- Podpora autentizace vůči LDAP (Active Directory).
- Programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9, IPFIX.
- Zpracování datového provozu IPv4 a IPv6, VLAN, MPLS a jejich reportování na kolektor.
- Monitorování provozu v tunelu GRE.
- Uživatelsky definovatelné šablony pro protokoly NetFlow v9 a IPFIX.
- Monitorování a reportování MAC adres ve flow statistikách. Možnost použít MAC adresu jako položku klíče flow záznamu.
- Detekce aplikací dle standardu NBAR2.
- Reportování RTT, SRT, delay, jitter, retransmise, out-of-order pakety jako součást flow statistik. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
- Monitorování a analýza DNS provozu - položky jako typ dotazu, dotazovaná doména, návratová hodnota, odpověď. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
- Monitorování DHCP provozu – položky jako typ DHCP požadavku, originální MAC adresa. Použití standardní technologie reportování těchto rozšiřujících statistik (šablony NetFlow v9 nebo IPFIX).
- Monitorování rozšířených L3/L4 informací - TTL (Time to live), TCP Window size, TCP SYN packet size umožňujících detekci NATů.
- Minimální kapacita paměti současných toků na sondě 500 tisíc toků per monitorovací port.
- Podpora pro nastavení časů u aktivní a neaktivní expirace toků.
- Podpora vzorkování na úrovni paketů. Podpora vzorkování na úrovni toků.
- Podpora simultánního exportu flow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě). Pro různé cíle exportu lze použít různé flow standardy (NetFlow v5, NetFlow v9, IPFIX).
- Podpora filtrování dat na sondě na základě IP prefixů, VLAN, AS (pro různé cíle exportu různé statistiky).
- Podpora pro nastavení hodnoty interface index pro exportované flow statistiky per monitorovací port.
- Servisní podpora na 3 roky garantovaná přímo výrobcem zařízení v režimu 24x7. Možnost otevírat servisní požadavky přímo u výrobce.

14) LOG Management – 1 ks

- HW appliance (montáž do běžného 19‘‘ datového rozvaděče, výška max. 1U) pro zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.
- Redundantní zdroje a ventilátory. Ventilátory za provozu vyměnitelné.
- 1x CPU min. 16 jader s podporou HyperThreadingu nebo Multi-Threadingu.
- Operační paměť RAM 64GB DDR-4
- 4x 1GbE RJ45 síťové rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému.
- Průměrný trvalý příjem událostí/s. (průměrná délka zprávy min. 700Byte) 2000 událostí/s
- Špičkový příjem bez ztráty dat po dobu nejméně 10 minut (průměrná délka zprávy min. 700 Byte) 4000 událostí/s
- Čistá velikost integrované databáze 12 TB
- Jedna webová console pro všechny administrátorské i operátorské činnosti
- Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200GB uložených událostí za den.
- Příjem a zpracování logů, události a další strojově generovaná data prostřednictvím protokolů SYSLOG (RFC3164, RFC5424, RFC5425), RELP
- Bezagentový sběr událostí, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů
- Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů.
- Windows agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému tzn., že musí být centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker.
- Windows agent musí podporovat centralizovanou konfiguraci Microsoft Sysmon pro obohacení logů, včetně globálního a selektivního zapínaní/vypínaní služby Sysmon a výběr z několika přednastavených konfigurací Sysmon v grafickém rozhraní centrální správcovské konzole systému.
- Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem.
- Windows agent musí podporovat sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem.
- Windows agent musí ke všem odesílaným událostem automaticky doplňovat jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K významným bezpečnostním událostem musí doplňovat značku a popis dle MITRE ATT&CK® matrice a k takto detekovaným procesům a souborům automaticky vytvářet SHA256 hash.
- Počet instalací Windows agenta nesmí být licenčně a časově omezen. Pokud je Windows agent licenčně nebo časově omezen, požadujeme dodání licencí na Windows agenty v množství 450 na dobu předpokládané morální životnosti produktu – min. 7 let.
- Výrobcem vytvářené parsery pro běžné systémy.
- Uživatelsky definované parsery - systém umožňuje dopsání parserů pro další zdroje log zařízení uživatelem pomocí tzv. vizuální programování, bez nutnosti spolupráce s výrobcem.

- Standardizace přijatých logů do jednotného formátu a jejich normalizace (rozdělení) do příslušných polí dle jejich typu. Vytvoření vlastního důvěryhodného časového razítka ke každému logu.
- Uchování originální verze přijatých logů/zpráv včetně původní časové značky události.
- Okamžitá a automatická indexace umožňující okamžité prohledávání událostí.
- Podporované formáty RAW, Syslog (RFC5424), CEF, LEEF, JSON (RFC8259)
- Systém nesmí umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. (ani libovolnou konfigurační změnou)
- Automatické doplňování reverzních DNS záznamů, čísel a jmen ASN systému a geolokace ke všem přijatým událostem a všem polím, obsahujícím IP adresy
- Nativní získávání logů z Office365 prostředí s licencí E3 bez nutnosti instalovat dodatečné externí komponenty
- Ověřování uživatele na externím LDAP serveru resp. ověření lokálního účtu v případě výpadku LDAP.
- Grafické rozhraní musí umožňovat filtraci nerelevantních událostí, snadné vyhledávání událostí, vytváření reportů a dynamickou vizualizaci událostí.
- Reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů
- Uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování
- Podpora základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity.
- Výrobcem předpřipravené sety/vzory alertů a korelací.
- Monitoring stavu systému - alertování při překročení prahových hodnot SMTP nebo Syslog
- REST-API pro integraci s externím monitorovacím systémem Zabbix, Nagios, MRTG
- Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba
- Dedikované síťové rozhraní pro management HW 1x 1GE RJ45
- Uživatelské role definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému
- Aktualizace systému přes centrální webovou správcovskou konzoli v jednom balíku.
- Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.
- Podpora komprese ukládaných dat
- Podpora důvěryhodného zálohování komprimovaných dat na externí systém.
- Servisní podpora na HW s opravou v místě instalace serveru, s garantovanou NBD od nahlášení závady 36 měsíců
- Servisní podpora na SW v rozsahu aktualizaci systému a parserů, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem 60 měsíců

Požadavky na implementaci:

- Montáž do racku
- Připojení do LAN infrastruktury
- Aktualizace FW a OS
- Napojení a sběr všech významných log zdrojů stávající a pořizované infrastruktury zadavatele – (firewally, LAN prvky, servery, OS, aplikace atd.)
- Nastavení reportingu
- Nastavení alertů
- Zaškolení obsluhy v rozsahu 1MD pro 2 osoby

Ověření kontroly funkčnosti systému:

- Základní nastavení systému a jeho konfigurace tak, aby mohl pracovat v prostředí zadavatele, včetně vytvoření uživatelů s rozdílným systémovým i databázovým oprávněním, a to v jednotném webovém rozhraní nabízeného systému
- Zapojení pěti vybraných zdrojových systémů logů odesílajících logy prostřednictvím Syslog protokolu přes UDP/TCP/TLS z prostředí zadavatele a otestování následujících vlastností:
    - nastavení klasifikace zdrojů
    - nastavení značek (tagů) pro vybrané zdrojové systémy
    - filtrování událostí
    - úprava normalizace existujícího zdroje v grafickém rozhraní nástroje
    - vytvoření reportů a exportu logů a vybraných údajů z logů
- Konfiguraci pěti vybraných systémů Microsoft Windows tak, aby posílaly EVTx a textové logy do testovaného systému, s konfigurací pouze v jednotném grafickém rozhraní nabízeného systému
- Ověření funkčních a výkonových parametrů Windows agenta a jeho centralizované správy v nabízeném systému včetně centrální instalace a centrální konfigurace Microsoft Sysmon služby pro rozšíření hodnoty logů vytvářených zdrojovými systémy dle doporučené auditní politiky.
- Konfigurace kolektoru logů z jedné databáze z prostředí zadavatele v jednotném webovém rozhraní nabízeného systému bez nutnosti instalovat na databázový server další produkty třetích stran
- Oprava ze záloh po simulovaném úplném selhání nabízeného systému v následujících krocích:
    - provedení zálohy konfigurace a dat na externí systém
    - vytažení dvou libovolných disků za běhu systému
    - nastavení systému do továrního nastavení
    - obnovení konfigurace a všech dat z vytvořených záloh
    - kontrola úplnosti obnovené konfigurace a dat ze záloh
- Navýšení a ponížení software nabízeného systému v grafickém rozhraní a provedení kontroly, že v případě ponížení nedojde ke ztrátě dříve shromážděných dat
- Kontrola, jakým způsobem se nastavuje systém ve vysoké dostupnosti (vytvoření clusteru) v jednotném webovém rozhraní systému a úplnost dokumentace k možným havarijním scénářům
- Kontrola výkonu systému v běžné zátěži – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající nabízenému systému, po dobu minimálně 30 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím skutečné době přijetí logu. Dále bude provedena kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musejí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR a geolokace.
- Kontrola výkonu systému v krátkodobém přetížení – generátorem logů se odešle vzorek originálních dat sesbíraných během předchozích testů. A to rychlostí odpovídající dvounásobku výkonu nabízeného systému po dobu 10 minut. Sledované hodnoty budou: přijetí všech logů a jejich správné zařazení do databáze s časovým razítkem odpovídajícím době přijetí logu systémem. Dále kontrola, zda nedošlo během zpracování logů k jejich poškození nebo ztrátě. Logy musejí být kompletně zpracovány bez ztráty dat, se správným časovým razítkem uloženy v databázi, normalizovány a doplněny o rozšiřující informace typu metadata, DNS-PTR, číslo a jméno ASN a geolokace.
    - Součástí ověření funkčních vlastností může být i ověření požadované funkcionality a parametrů dodaného systému dle Technické specifikace tohoto zadání.

- Ověření funkčních vlastností nabízeného systému bude provádět zadavatel, vycházeje z dokumentace k nabízenému systému. V případě nejasností zadavatel vyzve k účasti zástupce dodavatele, který mu poskytne potřebnou součinnost, a to maximálně do 3 pracovních dnů po doručení výzvy uchazeči. Testy budou provedeny v prostředí zadavatele.

15) Instalace a implementace – soubor

- Rozbalení veškerého dodaného HW, kontrola bezvadného stavu, likvidace přepravního a obalového materiálu a spolupráce s dodavatelem na evidenci HW (případné opatření evidenčními štítky);
- Instalace a zprovoznění veškerého dodaného HW do stávajících 19“ rozvaděčů a provedení funkčních testů;
- Instalace a zprovoznění veškerého dodaného SW na nově dodaný HW;
- Implementace zálohovacího SW v souladu s metodikou výrobce na odolnost diskových úložišť záloh před útoky ransomware;
- Nastavení LAN komponent tak, aby odpovídalo po konceptuální stránce stávajícímu schématu, tedy byly schopny rozšířit, popř. převzít, funkci původní infrastruktury, tj. tak, aby nastavení firewallu odpovídalo aktuálnímu stavu a switche byly zapojeny v patřičné topologii tak, aby umožňovaly serverům komunikaci nutnou k následující fázi konfigurace a zprovoznění nového produkčního prostředí;
- Zavedení veškerého dodaného HW do monitoringu dodavatele i objednatele;
- Instalace veškerého dodaného SW a jeho zavedení do monitoringu objednatele;
- Provedení výkonových testů pole
- Nastavení monitoringu zálohování na úroveň jednotlivých HW a SW složek zálohovacího řešení, zálohovacích úloh a jejich průběhu;
- V případě pochybností o výkonnostních parametrech dodaného řešení diskových polí může objednatel pro akceptaci této fáze požadovat výkonnostní test.
- Konfigurací a zprovozněním nového produkčního prostředí se rozumí především výstavba virtualizační platformy v obou lokalitách datového centra se samostatně funkčním managementem a síťovými službami se zprovozněním současných produkčních virtuálních serverů Jedná se zejména o následující úkony:
- Úprava konfigurace datového centra tak, aby stávající produkční prostředí a služby jím poskytované byly provozovány, monitorovány, zálohovány a zabezpečeny na nově dodaném HW a SW;
- Instalace prostředí MS Windows dle dodaných licencí pro servery v primární i sekundární lokalitě;
- Nastavení virtualizace tak, aby užívala primární a sekundární diskové pole včetně synchronní replikace dat mezi lokalitami;
- Plné zanesení virtualizace do monitoringu objednatele;
- Provedení testu výkonu spojení mezi jednotlivými komponentami a disaster recovery při zátěži pro vyloučení SPOF;
- Integrace zálohování s virtualizační konzolí;
- Požadujeme instalaci základního zálohovacího SW (řízení, správa)
- Požadujeme instalaci všech potřebných serverů pro transport dat (data moover, media server, proxy server)
- Pokud má backup SW oddělené GUI klienty pro správu, požadujeme ukázkovou instalaci takové admin konzole na OS Linux

- Pokud má backup SW oddělené zálohovací klienty pro zálohování daných OS, požadujeme ukázkovou instalaci na vybraných OS (Windows, Linux)
- Požadujeme backup SW integraci s administračními nástroji pro virtualizované prostředí MS Windows a VMware
- Požadujeme backup SW integraci s funkcí snapshotů s nabízeným diskovým polem
- Požadujeme zviditelnění a nakonfigurování všech uvažovaných cílů záloh (VTL zařízení, D2D zařízení)
- Požadujeme konfiguraci všech rozhraní (LAN/SAN) na všech serverech sloužících pro transport zálohovaných dat (data moover, proxy servery, media servery, storage servery)s optimalizací na a) HA (vysokou dostupnost) b) propustnost (agregace více linek)
- Na všech komponentách zálohovacího eko-systému implementovat administraci a přístupy s ohledem na RBAC (Role Based Access Control) včetně napojení na centrální AD/LDAP.
- Požadujeme vytvoření automatizovaného reportovacího systému, který bude informovat o nedokončených zálohovacích úlohách
- Požadujeme ukázku monitoringu:
    - stavy-statusy jednotlivých komponent (řídící serever, data moover, cíl záloh)
    - stavy-statusy úloh, statistiky úloh
    - kapacity, využité a volné kapacity v jednotlivých cílech záloh
- Požadujeme dodání elektronické dokumentace (pdf) ke všem použitým SW komponentám (user guide, admin guide, config guide atp.)
- Požadujeme vytvoření a předání dokumentace o konkrétním provedení a nastavení celého zálohovacího prostředí. (otevřený editovatelný formát ODF např. *.odt nebo MS Office formát např. *.docx)
- Požadujeme zajištění instalace prostředí MS Windows dle dodaných licencí pro servery v primární i sekundární lokalitě, integraci na primární a sekundární diskové pole včetně synchronní replikace dat mezi lokalitami
- Požadujeme logickou migraci stávajícího prostředí MS Windows do nového prostředí založeného na MS Windows nezbytnou pro konfiguraci nového produkčního prostředí
- Požadujeme fyzickou migraci a konsolidaci dat fyzických serverů a jejich logickou migraci nezbytnou pro konfiguraci nového produkčního prostředí
- Zanesení dokumentace prostředí do Redmine zadavatele, popř. předání formou dokumentů ve formátech odt, docx či pdf;
- Dokumentace jednotlivých HW a SW komponent musí mít část věnující se instalaci, konfiguraci, běžné administraci a užívání.
- Zkušební provoz je jedno (1) měsíční období navazující na úspěšnou akceptaci konfigurace a zprovoznění nového produkčního prostředí, v kterém je dodavatel povinen odstraňovat všechny známe i nově se vyskytnuvší vady a problémy bránící či komplikující běžný provoz nově dodaného HW a SW a IT služeb zadavatele.

16) Zaškolení obsluhy - soubor

- Zaškolení 2 zaměstnanců zadavatele v obsluze a údržbě zařízení v rozsahu 16 pracovních hodin na dodaném zařízení v místě plnění (s min. rozsahem 8 pracovních hodin na zařízení LOG management).

Č.	Kritérium	Splněno	Popis řešení
1.	Server vč. příslušenství	ANO	**2x HOST server** HPE DL380 Gen11 8SFF NC CTO, 1x procesor INTEL Xeon-G 6444Y CPU for HPE, 12x HPE 32GB 2Rx8 PC5-4800B-R Smart Kit, celkem 384GB RAM, HPE DL380 Gen11 2U 8SFF x1 TM Kit, 2x HPE SN1610E 32Gb 1p FC HBA, 1x BCM 57412 10GbE 2p SFP+ OCP3 Adapter, 1x BCM 5719 1Gb 4p BASE-T OCP Adapter, 2x HPE 800W FS Plat Ht Plg LH Power supply Kit, HPE iLO Adv 1-svr Lic 3yr Support, HPE DL360 Gen11 CPU1/OCP2 x8 Enable Kit, HPE DL380/DL560 G11 2U High Perf Fan Kit, HPE NS204i-u Gen11 Hott Plug Boot Option Device (2x 480 GB SSD), HPE DL380/DL560 G11 High Perf 2U HS Kit, HPE DL380 G11 NS204i-u Internal Cable Kit, HPE DL3XX Gen11 Easy Install Rail 3 Kit, záruka HPE TechCare 3Y Basic service, **1x management server** HPE DL380 Gen11 8SFF NC CTO, 1x procesor INTEL Xeon-G 6434 CPU for HPE, 4x HPE 32GB 2Rx8 PC5-4800B-R Smart Kit, celkem 128GB RAM, HPE DL380 Gen11 2U 8SFF x1 TM Kit, 2x HPE SN1610E 32Gb 1p FC HBA, 1x BCM 57412 10GbE 2p SFP+ OCP3 Adapter, 1x BCM 5719 1Gb 4p BASE-T OCP Adapter, 2x HPE 800W FS Plat Ht Plg LH Power supply Kit, HPE iLO Adv 1-svr Lic 3yr Support, HPE DL360 Gen11 CPU1/OCP2 x8 Enable Kit, HPE DL380/DL560 G11 2U High Perf Fan Kit, HPE NS204i-u Gen11 Hott Plug Boot Option Device (2x 480 GB SSD), HPE DL380/DL560 G11 High Perf 2U HS Kit, HPE DL380 G11 NS204i-u Internal Cable Kit, HPE DL3XX Gen11 Easy Install Rail 3 Kit, záruka HPE TechCare 3Y Basic service **1x záložní zdroj typ I,** APC Smart-UPS SRT 6000VA RM 230V, On-Line, 4U, Rack Mount (6000W) **1x záložní zdroj typ II**, APC Smart-UPS 3000VA LCD RM 2U 230V (2700W) with Network Card
2.	Zálohovací pásková knihovna	ANO	HPE pásková mechanika StoreEver MSL2024 Tape Library, 2x HPE StoreEver MSL LTO-8 Ultrium 30750 FC Drive Upgrade Kit, 2x HPE Premier Flex LC/LC Multi-mode OM4 2 Fiber 5m Cable, 2x HPE Ultrium Universal Cleaning Cartridge, 22x HPE LTO-8 Ultrium 30TB RW Data Cartridge, HPE 3Y Tech Care Basic Service, HPE MSL2024 Library Support
3.	Firewall	ANO	HA bundle 2x FortiGate 100F + 1x Licence UTP, 24x7 Unified Threat Protection 3 YEAR
4.	Diskové pole	ANO	2x diskové pole HP Alletra Storage MP Starter Kit systém obsahuje fixní konfiguraci dvou (2) řadičů, každého s 8-core AMD CPU a 256GB cache a 4-portovým Fibre Channel adaptérem (osazený 32 Gb SFP moduly). Diskové pole obsahuje 12x 3,84TB pevný disk NVMe SFF SSD, efektivní kapacita 77,2TB, užitná kapacita 30,9TB. Součástí je také subskripce HPE

Č.	Kritérium	Splněno	Popis řešení
			GreenLake for Block Storage včetně telefonické podpory 24x7 na zvolené období. Záruka 3 roky 24x7 Essential warranty.
5.	FC infrastruktura	ANO	**2x FC switch** HPE FC switch SN3600B 32Gb 24/8 Fibre Channel Switch, 2x HPE B-series 32Gb SFP28 Short Wave 8-pack Transceiver, HPE SN3600B 8-port Fibre Channel Upgrade E-LTU, 8x HPE Premier Flex LC/LC Multi-mode OM4 2 Fiber 5m Cable, HPE 3Y Tech Care Essential Service, HPE SN3600B 32Gb 24/8 FC Switch Support, **4x GBIC modul** HPE B-series 16Gb SFP+ Long Wave 10km Transceiver
6.	Switche - síťové přepínače LAN	ANO	**2x LAN Switch** Aruba 2930M 24G 1-slot Switch (JL319A), 2x Aruba X371 12VDC 250W AC Power Supply (JL085A), Power Cord - Europe localization, 1x Aruba 3810M/2930M 4SFP+ MACsec Module (JL083A),1x Aruba 2930 2-port Stacking Module (JL325A), 1x Aruba 2920/2930M 0,5m Stacking Cable (J9734A) **4x GBIC modul** Aruba 10G SFP+ LC LR 10km SMF Transceiver (J9151E)
7.	WiFi - bezdrátové prvky	ANO	**20x Aruba Access Point** AP-515 (RW) Unified AP **20x držák** HPE Aruba Networking AP-MNT-MP10-D
8.	NAC - Network Access Control	ANO	ClearPass perpetual licence , support 3 roky, 100 koncových zařízení Instalace, nastavení, konfigurace HPE ARUBA Clear Pass
9.	Sada licencí software	ANO	2x CSP Windows Server 2022 Datacenter - 16 Core 2x CSP Windows Server 2022 Standard - 16 Core" 150x CSP Windows Server 2022 - 1 User CAL 1x CSP Exchange Server Standard 2019 150x CSP Exchange Server Standard 2019 User CAL 2x SQL Server Standard Core SLng LSA OLV 2Core licence NL, 3Year minimální licencovaný počet: 4Core
10.	Zálohovací systém	ANO	Veeam Data Platform Essentials Universal Subscription License. Obsahuje 20ks zálohovaných VM, Includes Enterprise Plus Edition features. - 3 Year Subscription Upfront Billing & Production (24/7) Support - Public Sector

Č.	Kritérium	Splněno	Popis řešení
11.	Bezpečnostní software	ANO	180x ESET PROTECT ENTERPRISE On-Premise (antivir, antispam, sandbox, šifrování, EDR/XDR), 3 roky, sleva pro subjekty veřejné správy 20%
12.	2-faktorové ověřování	ANO	1x FortiToken HW, FortiToken-200B, FortiToken-200B-100, HW token pro 100 uživatelů 1x FortiTokenMobile (Electronic License), FortiTokenMobile FTM-ELIC-50, sw aplikace 50 uživatelů
13.	NDR - Network Detection and Response	ANO	Flowmon HW sonda, 10GbE, 1 místo sběru dat, 1TB databáze, 3 roky podpora 1x Příplatek na ADS lite
14.	LOG Management	ANO	LOGmanager verze M, 3y SW support included Nasazení a implementace od výrobce
15.	Instalace a implementace	ANO	Dle výše uvedených požadavků v plném rozsahu
16.	Zaškolení obsluhy	ANO	Zaškolení 2 zaměstnanců zadavatele v obsluze a údržbě zařízení v rozsahu 16 pracovních hodin na dodaném zařízení v místě plnění (s min rozsahem 8 pracovních hodin na zařízení LOG management).

Prohlašuji, že veškeré shora uvedené údaje (parametry) jsou úplné, pravdivé a odpovídají skutečnosti. Jsem si vědom/a právních následků v případě uvedení nesprávných nebo nepravdivých údajů (parametrů).

V Novém Městě nad Metují, dne .....

[redacted]

.....

Bc. David Línek, jednatel společnosti