Příloha č. 1

4. DOLOŽENÍ TECHNICKÉ SPECIFIKACE A GARANTOVANÝCH TECHNICKÝCH PARAMETRŮ PRO NABÍZENÝ PŘEDMĚT VEŘEJNÉ ZAKÁZKY

Technická specifikace předmětu veřejné zakázky

Zadavatel požaduje, aby Dodavatel vyplnil níže uvedené tabulky včetně uvedení přesného (konkrétního) označení nabízeného výrobku (produktu).

Aktivní síťový prvek – 10 identických kusů:
Označení nabízeného výrobku (produktu): **JUNIPER EX4400-48F**

	Specifikace minimálních požadavků stanovených Zadavatelem	Dodavatelem nabízený parametr/hodnota	Splněno (ano/ne)
Charakteristika:	• min. 12x10GbE SFP+, min. 36x 1GbE SFP, min. 4x 25GbE SFP28 jako extension, min. 2x 100GbE QSFP28 • dedikovaný out-of-band management interface RJ45, konzolový port (RJ45, USB, RS-232 9 pin) • existence varianty modelu podporující napájené porty (všechny porty) - PoE (IEEE 802.3af), PoE+ (IEEE 802.3at) a Fast PoE • maximální rozměr chassis prvku 1U, redundantní aktivní chlazení (vyměnitelné za běhu) • napájení 220V, umožňuje osazení dvěma zdroji (vyměnitelné za běhu)	• 12x10GbE SFP+, 36x 1GbE SFP, 4x 25GbE SFP28 jako extension, . 2x 100GbE QSFP28 • dedikovaný out-of-band management interface RJ45, konzolový port (RJ45, USB, RS-232 9 pin) • existence varianty modelu podporující napájené porty (všechny porty) - PoE (IEEE 802.3af), PoE+ (IEEE 802.3at) a Fast PoE • maximální rozměr chassis prvku 1U, redundantní aktivní chlazení (vyměnitelné za běhu) • napájení 220V, umožňuje osazení dvěma zdroji (vyměnitelné za běhu) • neblokující architektura o plné rychlosti portů pro L2/L3 min. 910 Gbps / 670 Mpps	Ano

	• neblokující architektura o plné rychlosti portů pro L2/L3 min. 910 Gbps / 670 Mpps • umožňuje seskupit přepínače do jednoho virtuálního síťového elementu (dále jako „VSE“) v rámci dostupných typů dané série přepínačů • VSE se chová jako jeden virtuální přepínač pro přístup pro správu, konfiguraci L2/L3, seznam a práce s porty apod. • jednotlivé přepínače tvořící VSE propojitelné na velkou vzdálenost pomocí optických kabelů a zabudovaných portů – minimálně 2km • do VSE je možno seskupit minimálně 9 přepínačů • VSE umožňuje redundantní komponentu/pravidla pro data • VSE umožňuje redundantní komponentu/pravidla pro řízení • přepínače ve VSE jsou vyměnitelné bez dopadu na zbytek hardware VSE • podpora fyzických rozhraní: 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 1000BASE-LH (nebo ZX), 10GBASE-SR, 10GBASE-LR, 10GBASE-T, 100GBASE-SR4, 100GBASE-LR4 • min. 110k MAC na systém, podpora paketů o délce 9k jako minimum • VLAN id rozsah 4k, konfigurovaných VLAN současně min. 4000 • IEEE 802.1Q (trunk intf.), VLAN vztažená na port, Hlasová VLAN, Privátní VLAN	• umožňuje seskupit přepínače do jednoho virtuálního síťového elementu (dále jako „VSE“) v rámci dostupných typů dané série přepínačů • VSE se chová jako jeden virtuální přepínač pro přístup pro správu, konfiguraci L2/L3, seznam a práce s porty apod • jednotlivé přepínače tvořící VSE propojitelné na velkou vzdálenost pomocí optických kabelů a zabudovaných portů – min. 2km • do VSE je možno seskupit minimálně 9 přepínačů • VSE umožňuje redundantní komponentu/pravidla pro data • VSE umožňuje redundantní komponentu/pravidla pro řízení • přepínače ve VSE jsou vyměnitelné bez dopadu na zbytek hardware VSE • podpora fyzických rozhraní: 1000BASE-T, 1000BASE-SX, 1000BASE-LX, 1000BASE-LH (nebo ZX), 10GBASE-SR, 10GBASE-LR, 10GBASE-T, 100GBASE-SR4, 100GBASE-LR4 • min. 110k MAC na systém, podpora paketů o délce 9k jako minimum • VLAN id rozsah 4k, konfigurovaných VLAN současně min. 4000 • IEEE 802.1Q (trunk intf.), VLAN vztažená na port, Hlasová VLAN, Privátní VLAN • umožňuje akceptovat non-tagged paket na trunk portu • LACP včetně LACP napříč stohem/VSE	

	• umožňuje akceptovat non-tagged paket na trunk portu • LACP včetně LACP napříč stohem/VSE • podpora automatické správy VLAN (GVRP, MVRP (IEEE 802.1ak) • xSTP (IEEE 802.1D/802.1s/802.1w), kompatibilní s PVST+ • BPDU guard, Loop protection, LLDP (IEEE 802.1AB), LLDP-MED (integrace s hlasovou VLAN) • MACsec (IEEE 802.1AE) – vyžadováno pro všechny 1/10 GB porty bez omezení • ACL implementovány v hardware bez dopadu na výkon • ACL definovatelné pro porty (vstup/výstup), VLAN, L3, podmínky pro shodu umožňují použít výrazy z L2-L4 OSI • ACL i pro IPv6, ACLka na provoz směrem k CPU, Policing / rate limit pro provoz směrem k CPU • L3 funkcionality podporováno v hardware s ohledem na výkon, L3 interface i pro VLAN • 130 000 IPv4 cest • 85 000 IPv6 cest • statické, dynamické směrování (OSPF, IS-IS, BGP, RIP) • virtuální směrování (VRF, směrovací instance) • DHCP server / relay • Multicast podporováno v hardware, IGMP snooping v 1/2/3 • podpora VRRP nebo ekvivalentní pro IPv6	• podpora automatické správy VLAN (GVRP, MVRP (IEEE 802.1ak) • xSTP (IEEE 802.1D/802.1s/802.1w), kompatibilní s PVST+ • BPDU guard, Loop protection, LLDP (IEEE 802.1AB), LLDP-MED (integrace s hlasovou VLAN) • MACsec (IEEE 802.1AE) – vyžadováno pro všechny 1/10 GB porty bez omezení • ACL implementovány v hardware bez dopadu na výkon • ACL definovatelné pro porty (vstup/výstup), VLAN, L3, podmínky pro shodu umožňují použít výrazy z L2-L4 OSI • ACL i pro IPv6, ACLka na provoz směrem k CPU, Policing / rate limit pro provoz směrem k CPU • L3 funkcionality podporováno v hardware s ohledem na výkon, L3 interface i pro VLAN • 130 000 IPv4 cest • 85 000 IPv6 cest • statické, dynamické směrování (OSPF, IS-IS, BGP, RIP) • virtuální směrování (VRF, směrovací instance) • DHCP server / relay • Multicast podporováno v hardware, IGMP snooping v 1/2/3 • podpora VRRP nebo ekvivalentní pro IPv6	

	• podpora OSPFv3, podpora IPv6 ACL • podpora DHCPv6 snooping, podpora IPv6 ND inspection, podpora IPv6 MLD snooping, IPv6 Route Advertisements (RA) Guard • 802.1x "single / multiple / single secured“ suplikant • 802.1x statický proskok, 802.1x VLAN assignment, 802.1x MAC radius, VoIP VLAN s 802.1x spoluprací • DHCP snooping, DHCP untrust porty, Dynamic ARP inspection • statická MAC / MAC omezení na port, limit na stěhování MAC • klasifikace provozu podporováno v hardware • klasifikace provozu na 802.1p, DSCP, IP precedence • klasifikace provozu na L2-L4 polích hlavičky paketu • tvarování egress portů, politika na ingress portech • min. 8x front unicast a min. 4 fronty multicast na port implementováno v hardware • podpora WDRR a SP • podpora WRED, Tail drop • vysoká dostupnost, modularita, VRRP • interface pro správu dostupný lokálně, telnet, SSH • autentifikace uživatelů (lokální, Radius, TACACS+) • automatická záloha konfigurace na remote SCP, FTP, TFTP,	• podpora OSPFv3, podpora IPv6 ACL • podpora DHCPv6 snooping, podpora IPv6 ND inspection, podpora IPv6 MLD snooping, IPv6 Route Advertisements (RA) Guard • 802.1x "single / multiple / single secured“ suplikant • 802.1x statický proskok, 802.1x VLAN assignment, 802.1x MAC radius, VoIP VLAN s 802.1x spoluprací • DHCP snooping, DHCP untrust porty, Dynamic ARP inspection • statická MAC / MAC omezení na port, limit na stěhování MAC • klasifikace provozu podporováno v hardware • klasifikace provozu na 802.1p, DSCP, IP precedence • klasifikace provozu na L2-L4 polích hlavičky paketu • tvarování egress portů, politika na ingress portech • min. 8x front unicast a min. 4 fronty multicast na port implementováno v hardware • podpora WDRR a SP • podpora WRED, Tail drop • vysoká dostupnost, modularita, VRRP • interface pro správu dostupný lokálně, telnet, SSH • autentifikace uživatelů (lokální, Radius, TACACS+) • automatická záloha konfigurace na remote SCP, FTP, TFTP, • umožňuje konfigurační změny přes txt soubor, podpora syslog (lokální i vzdálený)	

	• umožňuje konfigurační změny přes txt soubor, podpora syslog (lokální i vzdálený) • umožňuje scriptování (např. tcl, python nebo jinak), • podpora automatizace konfigurace a sběru dat pomocí frameworků • podpora bezzásahové prvotní konfigurace (Zero Touch Provisioning) • SNMP verze 1/2c/3, ping, traceroute, Flow technologie • zrcadlení provozu lokální i vzdálené • vynucení potvrzení změn nastavení • dostupný centrální management s GUI pro správu min. 100 přepínačů • všechny funkce přepínače konfigurovatelné plně bez výjimky jak prostřednictvím WWW rozhraní, tak i telnet na ssh serveru, to vše běžící přímo na přepínači bez nutnosti dalšího prostředníka a nutnosti kombinovat uvedená rozhraní	• umožňuje scriptování (např. tcl, python nebo jinak), • podpora automatizace konfigurace a sběru dat pomocí frameworků • podpora bezzásahové prvotní konfigurace (Zero Touch Provisioning) • SNMP verze 1/2c/3, ping, traceroute, Flow technologie • zrcadlení provozu lokální i vzdálené • vynucení potvrzení změn nastavení • dostupný centrální management s GUI pro správu min. 100 přepínačů všechny funkce přepínače konfigurovatelné plně bez výjimky jak prostřednictvím WWW rozhraní, tak i telnet na ssh serveru, to vše běžící přímo na přepínači bez nutnosti dalšího prostředníka a nutnosti kombinovat uvedená rozhraní	
Další příslušenství:	• Minimálně 48ks optických převodníků (4ks pro každý aktivní prvek) SFP+ (10Gbit/s.) kompatibilní s dodávaným přepínačem	• 48ks optických převodníků (4ks pro každý aktivní prvek) SFP+ (10Gbit/s.) kompatibilní s dodávaným přepínačem	Ano
Záruka a podpora:	• Produktová podpora výrobku spočívající ve výměně zařízení v případě jeho poruchy, získání nových verzí software a vytvoření „case“ technického rázu, po dobu min. 24 měsíců	• Produktová podpora výrobku spočívající ve výměně zařízení v případě jeho poruchy, získání nových verzí software a vytvoření „case“ technického rázu, po dobu min. 24 měsíců	Ano

Licence zálohovací vrstvy – 1 licence pokrývající 50 VM s minimální platností 36 měsíců:
Označení nabízeného výrobku (produktu): **Veeam Data Platform Foundation Universal Subscription License, 50VM , 3y**

	Specifikace minimálních požadavků stanovených Zadavatelem	Dodavatelem nabízený parametr/hodnota	Splněno (ano/ne)
Typ zálohovaní:	• Zálohovací software podporuje infrastrukturu založenou na komerčních hypervizorech. Všechny níže popsané funkcionality musí být splněny pro všechny zmíněné verze hypervizorů. • Software obsahuje podporu pro virtualizační servery spravované pomocí centrální správy i samostatné konzoly přímo na serveru, včetně dodávky integrační funkcionality. • Software obsahuje podporu pro zálohování všech operačních systémů, které jsou podporované pro provoz na výše zmíněných hypervizorových platformách. • Software musí být nezávislý na konkrétním výrobci hardware a jeho funkčnost nesmí být omezena na hardware platformu jednoho výrobce. • Software musí vytvářet soubory záloh, které jsou migrovatelné nezávisle na metadatech nebo databázi. • Software musí umožnit zálohu konfigurace celého zálohovacího prostředí pro případ rychlé reinstalace nebo migrace do DR prostředí. • Software musí disponovat vlastním deduplikačním mechanismem, nezávislým na hardwarové platformě pro ukládání dat.	• Zálohovací software podporuje infrastrukturu založenou na komerčních hypervizorech. Všechny níže popsané funkcionality musí být splněny pro všechny zmíněné verze hypervizorů. • Software obsahuje podporu pro virtualizační servery spravované pomocí centrální správy i samostatné konzoly přímo na serveru, včetně dodávky integrační funkcionality. • Software obsahuje podporu pro zálohování všech operačních systémů, které jsou podporované pro provoz na výše zmíněných hypervizorových platformách. • Software je nezávislý na konkrétním výrobci hardware a jeho funkčnost nesmí být omezena na hardware platformu jednoho výrobce. • Software vytváří soubory záloh, které jsou migrovatelné nezávisle na metadatech nebo databázi. • Software umožňuje zálohu konfigurace celého zálohovacího prostředí pro případ rychlé reinstalace nebo migrace do DR prostředí.	ano

	• Software musí umožňovat v rámci jedné zálohovací úlohy ukládání souborů záloh do více fyzických diskových úložišť s různým typem připojení a od různých výrobců pro usnadnění škálovatelnosti řešení. • Ztráta, poškození nebo nedostupnost jakékoliv databáze nesmí vést k nemožnosti obnovy dat ze souborů záloh. • Software nesmí vyžadovat instalaci a údržbu agentů uvnitř VM pro zálohování dat. • Software nesmí vyžadovat instalaci agentů ve VM pro proces obnovy dat aplikací. • Software musí umožňovat „single pass backup", kterým se rozumí schopnost vytvoření jednoho "univerzálního" souboru zálohy – s možností vyjmutí jednotlivých adresářů nebo souborů z procesu zálohy, umožňujícího obnovu jak celé VM, tak jednotlivých souborů nebo aplikačních položek. • Software musí umožňovat obnovu do původní i nové lokality a to jak pro celé VM, jednotlivé virtuální disky, tak pro jednotlivé soubory či objekty aplikací. • Software musí mít mechanismus pro notifikaci o průběhu záloh a chybách pomocí e-mail nebo SNMP. • Software musí umožnit definici pre- a post-backup skriptů a pre-freeze / post-thaw skriptů pro zajištění konzistence jakýchkoliv aplikací v	• Software disponuje vlastním deduplikačním mechanismem, nezávislým na hardwarové platformě pro ukládání dat. • Software umožňuje v rámci jedné zálohovací úlohy ukládání souborů záloh do více fyzických diskových úložišť s různým typem připojení a od různých výrobců pro usnadnění škálovatelnosti řešení. • Ztráta, poškození nebo nedostupnost jakékoliv databáze nesmí vést k nemožnosti obnovy dat ze souborů záloh. • Software nevyžaduje instalaci a údržbu agentů uvnitř VM pro zálohování dat. • Software nevyžaduje instalaci agentů ve VM pro proces obnovy dat aplikací. • Software umožňuje „single pass backup", kterým se rozumí schopnost vytvoření jednoho "univerzálního" souboru zálohy – s možností vyjmutí jednotlivých adresářů nebo souborů z procesu zálohy, umožňujícího obnovu jak celé VM, tak jednotlivých souborů nebo aplikačních položek. • Software umožňuje obnovu do původní i nové lokality a to jak pro celé VM, jednotlivé virtuální disky, tak pro jednotlivé soubory či objekty aplikací. • Software má mechanismus pro notifikaci o průběhu záloh a chybách pomocí e-mail nebo SNMP.	

	průběhu zálohy a pro integraci s produkty třetích stran. • Software musí poskytovat samoobslužný webový portál pro obnovu dat uživatelsky minimálně na úrovni celých VM, Guest OS souborů. • Software musí obsahovat přímou integraci s podporou pro virtuální servery včetně vCD metadat.	• Software umožňuje definici pre- a post- backup skriptů a pre-freeze / post-thaw skriptů pro zajištění konzistence jakýchkoliv aplikací v průběhu zálohy a pro integraci s produkty třetích stran. • Software poskytuje samoobslužný webový portál pro obnovu dat uživatelsky minimálně na úrovni celých VM, Guest OS souborů. • Software obsahuje přímou integraci s podporou pro virtuální servery včetně vCD metadat	
Možnosti obnovy:	• Software musí obsahovat obnovu Virtuálních Serverů přímo do cloudového i on-premis prostředí. • Software musí obsahovat samoobslužný portál pro zálohování a obnovu pro uživatele vCloud Directoru. • Software musí obsahovat šifrování celé síťové komunikace mezi všemi komponentami řešení bez dopadu na jiné funkcionality. • Software musí obsahovat šifrování zálohovacích souborů. • Software musí disponovat vlastní správou šifrovacích klíčů s řízením jejich expirace a mechanizmem obnovy v případě ztráty hesla k šifrovanému zálohovacímu souboru. • Software musí mít klient/server architekturu s možností instalace více instancí administrátorské konzole.	• Software obsahuje obnovu Virtuálních Serverů přímo do cloudového i on-premis prostředí. • Software obsahuje samoobslužný portál pro zálohování a obnovu pro uživatele vCloud Directoru. • Software obsahuje šifrování celé síťové komunikace mezi všemi komponentami řešení bez dopadu na jiné funkcionality. • Software obsahuje šifrování zálohovacích souborů. • Software disponuje vlastní správou šifrovacích klíčů s řízením jejich expirace a mechanizmem obnovy v případě ztráty hesla k šifrovanému zálohovacímu souboru. • Software má klient/server architekturu s možností instalace více instancí administrátorské konzole. • Software využívá výrobcem hypervisoru podporovanou technologii Change Block Trackingu (CBT).	ano

	• Software musí využívat výrobcem hypervisoru podporovanou technologii Change Block Trackingu (CBT). • Software musí být schopen řídit svou zátěž vůči jednotlivým produkčním datastorům. • Pokud navrhované řešení využívá k zálohování hypervizorový snapshot, musí mít mechanizmus ověření jeho odstranění a detekci “orphaned snapshots” a automaticky zajistit konsolidaci takových snapshotů. • Software musí podporovat obnovu ze snapshotů podporovaných diskových polí na identické úrovni, jako ze souborů záloh. • Software musí obsahovat možnost vytváření archivů záloh na páskové knihovny s podporou trackování VM na páskách. • Páskovou knihovnu musí být možné provozovat separátně od backup serveru. • Software musí obsahovat funkcionalitu vytváření kopií záloh do vzdálených lokalit přes WAN sítě. • Software musí obsahovat funkcionalitu vytváření dlouhodobé retenční politiky, minimálně na úrovni GFS (Grandfather-father-son) retenční politiky. • Software musí obsahovat podporu pro BlockClone API pro Windows Server 2016 a 2019 s ReFS file systémem jako backup repository.	• Software je schopen řídit svou zátěž vůči jednotlivým produkčním datastorům. • Navrhované řešení využívá k zálohování hypervizorový snapshot, má mechanizmus ověření jeho odstranění a detekci “orphaned snapshots” a automaticky zajistit konsolidaci takových snapshotů. • Software podporuje obnovu ze snapshotů podporovaných diskových polí na identické úrovni, jako ze souborů záloh. • Software obsahuje možnost vytváření archivů záloh na páskové knihovny s podporou trackování VM na páskách. • Páskovou knihovnu je možné provozovat separátně od backup serveru. • Software obsahuje funkcionalitu vytváření kopií záloh do vzdálených lokalit přes WAN sítě. • Software obsahuje funkcionalitu vytváření dlouhodobé retenční politiky, minimálně na úrovni GFS (Grandfather-father-son) retenční politiky. • Software obsahuje podporu pro BlockClone API pro Windows Server 2016 a 2019 s ReFS file systémem jako backup repository. • Software je schopen zálohovat jakoukoliv dostupnou konektivitou na zdrojovou infrastrukturu. Musí tedy podporovat všechny zálohovací transportní režimy podporované hypervisorem (network, hotadd, direct SAN, direct NFS).	

	• Software musí být schopen zálohovat jakoukoliv dostupnou konektivitou na zdrojovou infrastrukturu. Musí tedy podporovat všechny zálohovací transportní režimy podporované hypervisorem (network, hotadd, direct SAN, direct NFS). • Software musí mít možnost vytvářen „ad-hoc" zálohy mimo zálohovací plán, dostupný přímo z prostředí vSphere klienta. • Pro vyšší škálovatelnost a rychlost musí nabízené řešení podporovat paralelní zpracování VM a jejich virtuálních disků včetně možnosti paralelní obnovy. • Software musí umožňovat okamžitou obnovu více virtuálních strojů bez nutnosti kopírování dat na produkční datové úložiště z libovolného bodu obnovy. • VM spuštěné v režimu okamžité obnovy musí být možné migrovat on-line nezávisle na podpoře této funkce na straně hypervizoru. • Musí podporovat granulární obnovu Active Directory (jakýkoliv objekt, jakýkoliv atribut, obnova uživatelského účtu včetně hesla, GPO, AD configuration Partition) a integrovaných DNS záznamů. • Musí podporovat obnovu Microsoft SQL 2008 a novější (database s možností point-in-time recovery, obnova na úrovní tabulek a schémat). • Software musí podporovat granulární obnovu databází Oracle běžících nad Linux a Windows	• Software má možnost vytvářen „ad-hoc" zálohy mimo zálohovací plán, dostupný přímo z prostředí vSphere klienta. • Pro vyšší škálovatelnost a rychlost nabízené řešení podporuje paralelní zpracování VM a jejich virtuálních disků včetně možnosti paralelní obnovy. • Software umožňuje okamžitou obnovu více virtuálních strojů bez nutnosti kopírování dat na produkční datové úložiště z libovolného bodu obnovy. • VM spuštěné v režimu okamžité obnovy je možné migrovat on-line nezávisle na podpoře této funkce na straně hypervizoru. • Podporuje granulární obnovu Active Directory (jakýkoliv objekt, jakýkoliv atribut, obnova uživatelského účtu včetně hesla, GPO, AD configuration Partition) a integrovaných DNS záznamů. • Podporuje obnovu Microsoft SQL 2008 a novější (database s možností point-in-time recovery, obnova na úrovní tabulek a schémat). • Software podporuje granulární obnovu databází Oracle běžících nad Linux a Windows OS (obnova v režimu point-in-time, obnova tabulek). • Software umožňuje indexaci souborů z Microsoft Windows a Linux VM, která poskytuje vyhledávání souborů ze záloh.	

	OS (obnova v režimu point-in-time, obnova tabulek). • Software musí umožňovat indexaci souborů z Microsoft Windows a Linux VM, která poskytuje vyhledávání souborů ze záloh. • Software musí využívat mechanismus VSS zabudovaný v Microsoft Windows OS vždy, když je to možné. • Software musí umožnit obnovu VM z hardware snapshot z podporovaných diskových polí. • Software musí podporovat „reverse CBT" a direct SAN obnovy. • Software musí poskytovat možnost ověřování obnovitelnosti ze souborů záloh nebo snapshotů diskových polí, včetně funkční aplikační logiky, bez nutnosti kopírování. • Tuto verifikaci musí být možné spouštět v časovém plánu jako automatizovanou úlohu.	• Software využívá mechanismus VSS zabudovaný v Microsoft Windows OS vždy, když je to možné. • Software umožňuje obnovu VM z hardware snapshot z podporovaných diskových polí. • Software podporuje „reverse CBT" a direct SAN obnovy. • Software poskytuje možnost ověřování obnovitelnosti ze souborů záloh nebo snapshotů diskových polí, včetně funkční aplikační logiky, bez nutnosti kopírování. • Tuto verifikaci je možné spouštět v časovém plánu jako automatizovanou úlohu.	
Možnosti licencí:	• Licencování nabízeného řešení nesmí být závislé na objemu zálohovaných dat nebo objemu dat uložených v zálohách.	Licencování nabízeného řešení není závislé na objemu zálohovaných dat nebo objemu dat uložených v zálohách	Ano
Záruka a podpora:	• Záruka na software minimálně 36 měsíců včetně opravných verzí.	Záruka na software 36 měsíců včetně opravných verzí.	Ano

Licence antivirového systému – 900 identických licencí s minimální platností 36 měsíců:
Označení nabízeného výrobku (produktu): **ESET PROTECT Essential On-Prem, 900 licencí, 3 roky**

	Specifikace minimálních požadavků stanovených Zadavatelem	Dodavatelem nabízený parametr/hodnota	Splněno (ano/ne)
Požadavky na management konzoli antivirového řešení:	• Webová konzole. • Umožňuje instalaci na Windows i Linux. • Předpřipravená virtual appliance pro virtuální prostředí, cloudové prostřední i prostředí on-premise. • Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce. • Umožňuje probuzení klientů pomocí Wake On Lan. • Umožňuje konfiguraci virtual appliance přes webové rozhraní Webmin. • Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta. • Offline uplatňování politik a spouštění úloh při výskytu definované události (odpojení od sítě při nalezení škodlivého kódu). • Administrace v nejpoužívanějších jazycích včetně češtiny. • Umožňuje konfiguraci oprávnění administrátorů (správa pouze části infrastruktury, které konkrétnímu administrátorovi podléhá). • Zabezpečení přístupu do vzdálené správy pomocí 2FA. • Podpora štítků/tagování pro snazší správu a vyhledávání.	• Webová konzole. • Umožňuje instalaci na Windows i Linux. • Předpřipravená virtual appliance pro virtuální prostředí, cloudové prostřední i prostředí on-premise. • Server/proxy architektura pro síťovou pružnost – snížení zátěže při stahování aktualizací detekčních modulů výrobce. • Umožňuje probuzení klientů pomocí Wake On Lan. • Umožňuje konfiguraci virtual appliance přes webové rozhraní Webmin. • Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta. • Offline uplatňování politik a spouštění úloh při výskytu definované události (odpojení od sítě při nalezení škodlivého kódu). • Administrace v nejpoužívanějších jazycích včetně češtiny. • Umožňuje konfiguraci oprávnění administrátorů (správa pouze části infrastruktury, které konkrétnímu administrátorovi podléhá). • Zabezpečení přístupu do vzdálené správy pomocí 2FA.	ano

	• Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce. • Vzdálené získání zachyceného škodlivého souboru z klienta. • Detekce nespravovaných (rizikových) počítačů komunikujících na síti. • Instalace a odinstalace aplikací 3. stran. • Vyčítání informací o verzích softwaru 3. stran. • Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty). • Odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce. • Vzdálená odinstalace antivirového řešení 3. strany. • Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku. • Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy. • Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů. • Podpora SNMP Trap, Syslogu a qRadar SIEM. • Podpora instalace skriptem - *.bat, *.sh, *.ini (GPO, SSCM).	• Podpora štítků/tagování pro snazší správu a vyhledávání. • Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce. • Vzdálené získání zachyceného škodlivého souboru z klienta. • Detekce nespravovaných (rizikových) počítačů komunikujících na síti. • Instalace a odinstalace aplikací 3. stran. • Vyčítání informací o verzích softwaru 3. stran. • Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty). • Odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce. • Vzdálená odinstalace antivirového řešení 3. strany. • Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku. • Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy.	

	• Reportování stavu klientů chráněných jinými bezpečnostními programy. • Schopnost zaslat reporty a upozornění na e-mail. • Přidání zařízení do vzdálené správy pomocí: - synchronizace s Active Directory, - ručního přidání pomocí dle IP adresy nebo názvu zařízení, - síťového skenu nechráněných zařízení v síti.	• Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů. • Podpora SNMP Trap, Syslogu a qRadar SIEM. • Podpora instalace skriptem - *.bat, *.sh, *.ini (GPO, SSCM). • Reportování stavu klientů chráněných jinými bezpečnostními programy. • Schopnost zaslat reporty a upozornění na e-mail. • Přidání zařízení do vzdálené správy pomocí: - synchronizace s Active Directory, - ručního přidání pomocí dle IP adresy nebo názvu zařízení, - síťového skenu nechráněných zařízení v síti.	
Požadavky na platformu antivirového řešení:	• Podporované klientské platformy - OS: Windows, Linux, MacOS, Android - vše v českém jazyce. • Podporované serverové platformy - OS: Windows, Linux - vše v českém jazyce. • Nativní podpora ARM64 architektury pro platformy Windows a MacOS. • Podpora technologie Intel Threat Detection Technology pro rychlejší odhalení hrozeb typu ransomware. • Antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb. • Modul pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost	• Podporované klientské platformy - OS: Windows, Linux, MacOS, Android - vše v českém jazyce. • Podporované serverové platformy - OS: Windows, Linux - vše v českém jazyce. • Nativní podpora ARM64 architektury pro platformy Windows a MacOS. • Podpora technologie Intel Threat Detection Technology pro rychlejší odhalení hrozeb typu ransomware. • Antimalware, antiransomware, antispyware a anti-phishing pro aktivní ochranu před všemi typy hrozeb.	Ano

	zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory. • Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému. • Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb. • Systém pro blokaci exploitů zneužívajících zero-day 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. • Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS). • Anti-phishing se schopností detekce homoglyph útoků. • Kontrola RAM paměti pro detekci malwaru využívající obfuskaci a šifrování. • Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů.	• Modul pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory. • Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému. • Aktivní i pasivní heuristická analýza pro detekci dosud neznámých hrozeb. • Systém pro blokaci exploitů zneužívajících zero-day 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. • Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS). • Anti-phishing se schopností detekce homoglyph útoků. • Kontrola RAM paměti pro detekci malwaru využívající obfuskaci a šifrování.	

	• Kontrola souborů v průběhu stahování pro snížení celkového času kontroly. • Kontrola souborů při zapisování na disku a extrahování archivačních souborů. • 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. • Modul behaviorální analýzy pro detekce chování 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 rootkitů obvykle se maskujících za součásti operačního systému. • Skener firmwaru BIOSu a UEFI. • Skenování souborů v cloudu OneDrive. • Funkcionalita pro klienty MS Windows – Antimalware, Antispyware, Personal IPS, Application control, Device control, Security Memory (zabraňuje útokům na běžící aplikace), kontrola integrity systémových komponent.	• Cloud kontrola souborů pro urychlení skenování fungující na základě reputace souborů. • Kontrola souborů v průběhu stahování pro snížení celkového času kontroly. • Kontrola souborů při zapisování na disku a extrahování archivačních souborů. • 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. • Modul behaviorální analýzy pro detekce chování 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 rootkitů obvykle se maskujících za součásti operačního systému. • Skener firmwaru BIOSu a UEFI. • Skenování souborů v cloudu OneDrive. • Funkcionalita pro klienty MS Windows – Antimalware, Antispyware, Personal IPS, Application control, Device control, Security Memory (zabraňuje útokům na běžící aplikace), kontrola integrity systémových komponent.	

	• Funkcionalita pro klienty MacOS – Device control, autoupgrade. • Umožňuje aplikování bezpečnostních politik i v offline režimu na základě definovaných podmínek. • Ochrana proti pokročilým hrozbám (APT) a 0-day zranitelnostem. • Podpora automatického vytváření dump souborů na stanici na základě nálezů. • Okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze) • 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). • Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP. • Umožňuje zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích.	• Funkcionalita pro klienty MacOS – Device control, autoupgrade. • Umožňuje aplikování bezpečnostních politik i v offline režimu na základě definovaných podmínek. • Ochrana proti pokročilým hrozbám (APT) a 0-day zranitelnostem. • Podpora automatického vytváření dump souborů na stanici na základě nálezů. • Okamžité blokování/mazání napadených souborů na stanici (s možností stažení administrátorem k další analýze) • 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). • Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP. Umožňuje zablokování konkrétní IP adresy po sérii neúspěšných pokusů o přihlášení pro protokoly SMB a RDP s možností výjimek ve vnitřních sítích.	
Další podmínky:	• Technická podpora v češtině. • Kanály pro řešení technických potíží (support) přes: - telefon, - e-mail, - chat, - support fórum.	• Technická podpora v češtině. • Kanály pro řešení technických potíží (support) přes: - telefon, - e-mail, - chat, - support fórum.	Ano

	• Technická podpora 12/5 poskytující pomoc na telefonu / přes e-mail / vzdáleně.	• Technická podpora 12/5 poskytující pomoc na telefonu / přes e-mail / vzdáleně.	
Záruka a podpora:	Záruka na software na minimálně 36 měsíců včetně opravných verzí.	• Záruka na software na minimálně 36 měsíců včetně opravných verzí.	Ano

Kompletní implementace vč. instalace, kabeláže, zaškolení:
Dodávka musí tvořit jeden kompletní funkční celek napojený na stávající infrastrukturu, včetně nespecifikovaného drobného materiálu a kabeláže vyplývajícího z konkrétně nabídnutého řešení. Součástí instalace bude sada optické a metalické kabeláže pro propojení soustavy aktivních prvků a další nespecifikované propojovací optické a metalické kabely v délce a počtu nezbytném pro úplné a bezvadné zapojení.

Součástí této položky je i implementace dodaného zboží:
Součástí této položky je i je realizace všech nezbytných prací souvisejících s konfigurací, instalací a propojením všech komponent do jednoho integrovaného, plně funkčního celku a propojení se stávající sítí dle požadavků specifikovaných touto Dokumentací.

Implementace HW:	• Montáž a zapojení HW dle aktuálního požadavku Zadavatele • Upgrade a sjednocení verze firmware ve všech zařízeních • Konfigurace LAN aktivních prvků - nedílnou součástí je instalace a konfigurace zařízení dle specifikace Zadavatele pro IPv4 a IPv6 L3 napojení na páteřní strukturu vyšší organizační jednotky a serverovou farmu
Implementace SW:	• Instalace a konfigurace prostředí pro OS virtualizaci včetně instalace management nástroje • Konfigurace zálohování a tvorby zálohovacího plánu • Zaškolení správce Zadavatele v prostředí centrální administrace antivirového řešení

Součástí této položky je i je realizace úvodního zaškolení obsluhy:
Dále je součástí dodávky tvorba předávací dokumentace a školení obsluhy na veškeré využité technologie v délce min. 5 pracovních dnů. Akceptační podmínky, tj. podmínky pro ověření funkčnosti všech instalovaných komponent v rámci instalace:

Funkce:
Dostupnost aplikací při simulovaném výpadku přepínače
Dostupnost aplikací při simulovaném výpadku napájení
Provedení obnovy dat dle zadání
Zobrazení simulovaného výpadku na instalované infrastruktuře v monitorovacím systému

Popis stávajícího stavu a další požadavky na řešení:
V současnosti je v lokalitě Pedagogické fakulty UP v Olomouci na Žižkově náměstí 5 provozována počítačová síť v následující struktuře:

- 1 x centrální rozvaděč osazený aktivními prvky, které určuje standard například jako Juniper QFX5110 (páteřní) a Juniper EX3400
- 3 x podružný rozvaděč osazený aktivními prvky které určuje standard například jako Juniper QFX5110 (páteřní) a Juniper EX3400 s PoE i bez

Nabízené řešení tedy musí umožnit propojení stávajícího řešení v areálu Pedagogické fakulty UP v Olomouci na Žižkově náměstí 5 s dodávanými prvky a technologiemi bez dalších dodatečných nákladů, se 100 % kompatibilitou a plnou redundancí, včetně zajištění plné propustnosti počítačové sítě.

5. CENOVÁ NABÍDKA

Název	Počet ks	Cena za ks bez DPH	Cena celkem bez DPH	DPH 21%	Cena celkem s DPH
JUNIPER EX4400-48F	10	71 200,00 Kč	712 000,00 Kč	149 520,00 Kč	861 520,00 Kč
Veeam Data Platform Foundation Universal Subscription License. Includes Enterprise Plus Edition features. 3 Years Renewal Subscription Upfront Billing & Production (24/7) Support. 50 instance pack. EDU	1	225 330,00 Kč	225 330,00 Kč	47 319,30 Kč	272 649,30 Kč
900 licencí ESET PROTECT Essential On-Prem, 3 roky	1	481 050,00 Kč	481 050,00 Kč	101 020,50 Kč	582 070,50 Kč
Instalace, implemantace, zaškolení	1	40 000,00 Kč	40 000,00 Kč	8 400,00 Kč	48 400,00 Kč
C e l k e m			**1 458 380,00 Kč**	**306 259,80 Kč**	**1 764 639,80 Kč**