1 Technická specifikace kupujícího

Zadavatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci.

Musí se jednat o zařízení nová, nepoužitá, nerepasovaná a určená pro prodej v České republice.

Součástí dodávky níže uvedených technologií budou i dále uvedené služby.

Součástí dodávky bude dále dodávka dokumentace a nezbytné zaškolení administrátorů v prostředí kupujícího k běžnému provozu a ovládání dodaných technologií včetně specifik a konfigurace provedené v prostředí kupujícího.

Nabízené zboží musí být standardní, běžně dostupné a určené k produkčnímu použití.

Není dovoleno použití beta-verzí, kódu s custom úpravami či neoficiálních verzí.

Veškeré nabízené zboží musí být pokryto oficiálním supportem, přičemž požadavek na provedení bezplatného servisního zásahu musí být možné kdykoliv vznést přímo na výrobce zařízení.

Veškeré deklarované funkce a technické parametry nabízeného zboží musí být dostupné nejpozději dnem podání nabídky.

Deklarované funkce a technické parametry nabízeného zboží musí být ověřitelné prostřednictvím oficiálních datasheetů, release notes či manuálů vydaných výrobcem.

Užité pojmy níže:

- NBD – další pracovní den, tzn. například realizace opravy zařízení nejpozději další pracovní den od nahlášení
- x BD – x pracovních dnů, tzn. například realizace opravy zařízení nejpozději poslední pracovní den dané lhůty od nahlášení
- on-site – realizace například opravy zařízení v místě dodávky

Z důvodu kompatibility se stávající infrastrukturou a proškolených správců počítačové sítě, mohou být v zadávací dokumentaci uvedeny konkrétní značky výrobků, nebo určitý výrobce. Tyto důvody jsou vždy uvedeny v konkrétní části specifikace tam, kde dochází k uvedení konkrétního produktového názvu. V souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zadavatel připouští možnost dodávky rovnocenného řešení, které však musí zajistit celý komplex služeb, který je kompatibilitou vyžadován, tedy komplexní řešení agendových informačních systémů nad touto platformou vybudovaných a provozovaných, které předmětnou infrastrukturu užívají a slouží k výkonu veřejné správy zadavatele.

V některých částech Přílohy č. 1 ZD – Technická specifikace jsou označeny konkrétními názvy některé přístroje, software a technologie, které v současné době využívá, a pro které požaduje s nově pořizovanými přístroji plnou kompatibilitu, a to z důvodu ochrany předchozích investic zadavatele a využitelnosti těchto přístrojů. Jedná se tedy o konkrétní označení stávajících zadavatelem využívaných přístrojů, se kterými požaduje kompatibilitu (nikoliv o označení výrobků, které mají být předmětem dodávky).

Obsah

2 Produkční server s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Základní a výkonová specifikace	**Typ zařízení**
	Server v provedení k instalaci do 19" racku, maximálně 2U.
	Barevně označené hot-plug vnitřní komponenty.
	Pro přístup ke všem komponentám není nutné nářadí.
	Zásuvné ližiny s managementem kabeláže.
	Procesor
	1ks CPU – architektura x86 s maximálně 16 plnohodnotnými jádry. V testu „Average CPU Mark“ dle databáze na cpubenchmark.net minimálně 52000 bodů (bodový stav k datu vyhlášení této VZ). Pro ověření musí být ve veřejně dostupné databázi uvedeno konkrétní modelové označení procesoru s příslušným skóre. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 jader z důvodu licencování hypervisoru, OS a aplikací.
	Paměť
	512GB, typu DDR5 s taktem 4800MT/s, Dual Rank; s ohledem na budoucí rozšiřitelnost s možností ponechání dodaných modulů požadujeme osadit moduly o minimální kapacitě 64 GB.
	Server musí umožnit rozšiřitelnost paměti na celkovou kapacitu min. 3 TB.
	Paměť serveru musí podporovat režim Fault Resilient Memory ve VMware ESX.
	Disky
	Možnost interního USB rozhraní s podporou zavádění hypervisoru.
	Osazení hotplug M.2 NVMe SSD, podpora RAID1 na úrovni hardware. Požadujeme osadit 2x 960GB.
	HBA
	Dvouportový 32GB Fibre Channel HBA kompatibilní s dodávaným diskovým polem podle této specifikace.
	Optické propojovací kabely MM v délce 3m pro redundantní připojení serverů k diskovému poli.
	LAN konektivita
	2 porty LAN 25 GbE SFP28.
	Dodávka včetně 2 MM zářičů 10/25 Gb (kompatibilita s dodávanými Ethernet adaptéry), 2 ks MM zářičů 10/25 Gb (kompatibilita s nabízenými switchi) a 2 ks 10 m MM optických kabelů LC/PC-LC/PC.
	Napájení
	2 ks zdroje napájení o výkonu zdroje min. 1100W, účinnost ve spektru výkonu poskytovaném serveru musí dosáhnout při 50% zátěži min. 96 %.
	Interface
	Min. 3x externí USB, z toho min. 1x USB 3.0

	Dedikovaný USB management port. Min. 1x VGA port. Sériový port. Stavové LED na čelním panelu (disky, teplota, napájení, paměť, PCIe).
Kompatibilita	- Microsoft® Windows Server®. - VMware® ESXi®.
Další požadované funkcionality	Změna řízení (zakázání/povolení) USB portů za běhu operačního systému bez rebootu serveru.
	Čelní kryt s LCD.
	Připojení na cloudový analytický portál výrobce serveru.
	Bezpečné vymazání konfigurace serveru, včetně NVMe SSD.
	Bezpečnostní funkce Secure Boot OS (MS Windows, VMware).
	Bezpečnostní aplikace, sloužící k ověření, že mezi expedicí zařízení od výrobce a jeho zprovozněním v datovém centru, nedošlo k neautorizovanému zásahu do FW či HW, ani k výměně libovolné klíčové komponenty za jinou.
Management a monitoring	Vyžadována je schopnost monitorovat a spravovat server out-of-band (OOB) bez nutnosti instalace agenta do operačního systému.
	Dedikovaný management Ethernet a USB port.
	Možnost vzdáleného přístupu přes dedikovaný nebo sdílený Ethernet port.
	Centrální management serverů musí umožňovat „server bare metal“ deployment založený na šablonách (předdefinovaných konfiguracích pravidel, jejichž součástí je kromě samotného OS i konfigurace BIOS, RAID, LAN, MAC, WWN). Z bezpečnostních důvodů musí být možné naplánovat pravidelné provedení porovnání aktuálního stavu konfigurace serveru s aplikovanou šablonou automatizovaným způsobem, s automatickým zasláním reportu o výsledku porovnání emailem. je-li tato vlastnost licencována, požadujeme plnou licenci v ceně serveru.
	Management serveru musí být integrovatelný do VMware vCenter serveru s plnou podporou správy a updatováni firmware serveru z prostředí vCenter serveru a s podporou vSphere Lifecycle Manager.
	Webové rozhraní HTML5.
	Konfigurace a monitorování přes mobilní aplikaci přes rozhraní BLE a/nebo WiFi.
	Přístup na OOB management pomocí protokolů IPMI 2.0, DCMI 1.5, CLI, SSH, Telnet, SMASH-CLP, WSMAN, Redfish, COM port.
	Přímé připojení OOB do operačního systému přes interní LAN nebo USB.
	Vzdálený update systému přes NFS v4, SMB 3.0 (NTLMv1 a NTLMv2).
	Zabezpečení uživatelů, integrace s LDAP, Active Directory.
	Bezpečný boot s podporou Secure UEFI včetně správy certifikátů.
	Možnost uzamčení systému proti instalaci upgradů.
	Uživatelsky konfigurovatelné logo úvodní stránky.
	Možnost spravovat více serverů z jednoho místa bez nutnosti instalace dalšího software.
	Přístup na konzoli serveru přes IP s podporou HTML5.

	Připojení vzdálených médií včetně share nebo image.
	Správa napájení včetně omezení příkonu.
	Automatické zasílání upozornění přes SNMPv1, SNMPv2, SNMPv3 a email.
	Monitorování stavu hardware (napájení, ventilátory, CPU, paměti, řadiče diskových polí, síťové porty, disky).
	Import a export serverových profilů.
	Vestavěná diagnostika.
	Bezpečné resetování všech komponent serveru a uvedení do počáteční konfigurace, včetně vymazání dat na discích.
	Logování na vzdálený server (Syslog).
	Konfigurace, update software, instalace operačního systému, diagnostika pomocí jediného nástroje bez nutnosti instalace dalších aplikací.
	Možnost správy více serverů z jedné konzole (1-to-many) bez nutnosti instalace dalších softwarových nástrojů.
	Automatický update z FTP serveru výrobce hardware.
Záruka a technická podpora	Záruka a záruční servis v délce min. 36 měsíců s reakční dobou na založený incident do konce následujícího pracovního dne (NBD).
	Technická podpora poskytovaná výrobcem serveru, nebo jeho autorizovaným zastoupením s přístupem k telefonické podpoře 24x7x365.
	Servis je poskytován výrobcem serveru nebo jeho autorizovaným zastoupením.
	Možnost stažení ovladačů a management software na webových stránkách výrobce.
	Zdarma aktualizace firmware min. po dobu platné podpory.
	Možnost automatického generování servisního incidentu přímo u výrobce hardware.

3 Zálohovací server s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Základní a výkonová specifikace	**Typ zařízení**
	Server v provedení k instalaci do 19" racku, maximálně 2U.
	Barevně označené hot-plug vnitřní komponenty.
	Pro přístup ke všem komponentám není nutné nářadí.
	Zásuvné ližiny s managementem kabeláže.
	Procesor
	1 ks CPU – architektura x86 s maximálně 16 plnohodnotnými jádry. V testu „Average CPU Mark“ dle databáze na cpubenchmark.net minimálně 40000 bodů (bodový stav k datu vyhlášení této VZ). Pro ověření musí být ve veřejně dostupné databázi uvedeno konkrétní modelové označení procesoru s příslušným skóre. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 jader z důvodu licencování hypervisoru, OS a aplikací.
	Paměť
	128 GB, typu DDR5 s taktem 4800MT/s, Dual Rank; s ohledem na budoucí rozšiřitelnost s možností ponechání dodaných modulů požadujeme osadit moduly o minimální kapacitě 64 GB.

	Diskový řadič
	x8 PCI Express Gen4. Typu SAS, dvoukanálový, až 32 zařízení. Podpora RAID 0, 1, 5, 6, 10, 50, 60. Podpora 6/12Gbps technologie rozhraní disků, 12Gbps na port. Podpora Non-RAID (Pass-through). Podpora Online Capacity Expansion (OCE). Podpora Online RAID Level Migration (RLM). Podpora Auto resume po ztrátě napájení. Podpora disků s formátem bloku 512n/512e/4Kn. Podpora TRIM/UNMAP příkazů pro SAS/SATA SSDs. Podpora NVRAM "Wipe". Podpora End Device Frame Buffering (EDFB). Podpora šifrování dat na discích (SED). Přímý přístup na SSD. Podpora až 64 logických disků. Podpora DDF, uložení konfigurace na discích (COD). Podpora S.M.A.R.T. Podpora globálního i dedikovaného hot-spare. Minimálně 8GB cache, zálohované akumulátorem. Volba režimu RAID nebo HBA.
	Prostředí pro OS
	Osazení hotplug M.2 NVMe SSD, podpora RAID1 na úrovni hardware. Požadujeme osadit 2x 960GB.
	Diskový subsystém
	Min. 12x3,5" pozice pro rotační disky a/nebo SSD s protokolem SAS/NLSAS/SATA. Požadujeme osadit min. 8 ks 20 TB SAS HOTSWAP.
	HBA
	Dvouportový 32GB Fibre Channel HBA kompatibilní s dodávaným diskovým polem.
	Optické propojovací kabely MM v délce 3m pro redundantní připojení serveru k diskovému poli.
	Externí datové porty
	2 porty externí SAS 12Gbps.
	LAN konektivita
	2 porty LAN 25 GbE SFP28.
	Dodávka včetně 2 MM zářičů 10/25 Gb (kompatibilita s dodávanými Ethernet adaptéry), 2 ks MM zářičů 10/25 Gb (kompatibilita s nabízenými switchi) a 2 ks 10 m MM optických kabelů LC/PC-LC/PC.
	Napájení

	2 ks zdroje napájení o výkonu zdroje min. 1100W, účinnost ve spektru výkonu poskytovaném serveru musí dosáhnout při 50% zátěži min. 96 %.
	Interface
	Min. 3x externí USB, z toho min. 1x USB 3.0. Dedikovaný USB management port. Min. 1x VGA port. Sériový port. Stavové LED na čelním panelu (disky, teplota, napájení, paměť, PCIe).
Kompatibilita	- Microsoft® Windows Server®. - VMware® ESXi®.
Další požadované funkcionality	Změna řízení (zakázání/povolení) USB portů za běhu operačního systému bez rebootu serveru.
	Čelní kryt s LCD.
	Připojení na cloudový analytický portál výrobce serveru.
	Bezpečné vymazání konfigurace serveru, včetně NVMe SSD.
	Bezpečnostní funkce Secure Boot OS (MS Windows, VMware).
	Bezpečnostní aplikace, sloužící k ověření, že mezi expedicí zařízení od výrobce a jeho zprovozněním v datovém centru, nedošlo k neautorizovanému zásahu do FW či HW, ani k výměně libovolné klíčové komponenty za jinou.
Management a monitoring	Vyžadována je schopnost monitorovat a spravovat server out-of-band (OOB) bez nutnosti instalace agenta do operačního systému.
	Dedikovaný management Ethernet a USB port.
	Možnost vzdáleného přístupu přes dedikovaný nebo sdílený Ethernet port.
	Centrální management serverů musí umožňovat „server bare metal“ deployment založený na šablonách (předdefinovaných konfiguracích pravidel, jejichž součástí je kromě samotného OS i konfigurace BIOS, RAID, LAN, MAC, WWN). Z bezpečnostních důvodů musí být možné naplánovat pravidelné provedení porovnání aktuálního stavu konfigurace serveru s aplikovanou šablonou automatizovaným způsobem, s automatickým zasláním reportu o výsledku porovnání emailem. je-li tato vlastnost licencována, požadujeme plnou licenci v ceně serveru.
	Webové rozhraní HTML5.
	Konfigurace a monitorování přes mobilní aplikaci přes rozhraní BLE a/nebo WiFi.
	Přístup na OOB management pomocí protokolů IPMI 2.0, DCMI 1.5, CLI, SSH, Telnet, SMASH-CLP, WSMAN, Redfish, COM port.
	Přímé připojení OOB do operačního systému přes interní LAN nebo USB.
	Vzdálený update systému přes NFS v4, SMB 3.0 (NTLMv1 a NTLMv2).
	Zabezpečení uživatelů, integrace s LDAP, Active Directory.
	Bezpečný boot s podporou Secure UEFI včetně správy certifikátů.
	Možnost uzamčení systému proti instalaci upgradů.
	Uživatelsky konfigurovatelné logo úvodní stránky.
	Možnost spravovat více serverů z jednoho místa bez nutnosti instalace dalšího software.

	Přístup na konzoli serveru přes IP s podporou HTML5.
	Připojení vzdálených médií včetně share nebo image.
	Správa napájení včetně omezení příkonu.
	Automatické zasílání upozornění přes SNMPv1, SNMPv2, SNMPv3 a email.
	Monitorování stavu hardware (napájení, ventilátory, CPU, paměti, řadiče diskových polí, síťové porty, disky).
	Import a export serverových profilů.
	Vestavěná diagnostika.
	Bezpečné resetování všech komponent serveru a uvedení do počáteční konfigurace, včetně vymazání dat na discích.
	Logování na vzdálený server (Syslog).
	Konfigurace, update software, instalace operačního systému, diagnostika pomocí jediného nástroje bez nutnosti instalace dalších aplikací.
	Možnost správy více serverů z jedné konzole (1-to-many) bez nutnosti instalace dalších softwarových nástrojů.
	Automatický update z FTP serveru výrobce hardware.
Záruka a technická podpora	Záruka a záruční servis v délce min. 36 měsíců s reakční dobou na založený incident do konce následujícího pracovního dne (NBD).
	Technická podpora poskytovaná výrobcem serveru, nebo jeho autorizovaným zastoupením s přístupem k telefonické podpoře 24x7x365.
	Servis je poskytován výrobcem serveru nebo jeho autorizovaným zastoupením.
	Možnost stažení ovladačů a management software na webových stránkách výrobce.
	Zdarma aktualizace firmware min. po dobu platné podpory.
	Možnost automatického generování servisního incidentu přímo u výrobce hardware.

4 Licence SW serverového operačního systému a klientské licence k němu

Je požadována dodávka následujících licencí:

Počet	Typ licence
2	Microsoft Windows Server Datacenter 2025 v rozsahu k pokrytí dodaných procesorových core v každém serveru pro hyperkonvergovanou infrastrukturu (HCI server) dle této specifikace, tedy pro všechna jádra procesů osazených v rámci produkčních serverů podle této specifikace.
1	Microsoft Windows Server Standard 2025 v rozsahu k pokrytí dodaných procesorových core v zálohovacím serveru pro dle této specifikace, tedy pro všechna jádra procesů osazených v rámci zálohovacího serveru podle této specifikace.
50	Microsoft Windows Server CAL 2025 - per User.
50	Microsoft Windows Server RDS CAL 2025 – per User.

Je požadována dodávka licencí, jejichž pravost je garantovaná a ověřitelná u vlastníka autorských práv MICROSOFT.

Dodavatel zároveň poskytne dokumentaci, ze které bude jasný původ, resp. prodejní kanál licencí nebo zajistí zpracování smlouvy se společností Microsoft (Microsoft – SELECT Plus, Open, CSP, MPSA, EA) ve prospěch kupujícího.

Vyžaduje se dodání licencí formou licenčního portálu vázaného na koncového zákazníka (kupujícího), jehož součástí budou:

- Seznam nabízených licencí a jejich počet,
- Instalační médium,
- Instalační klíče,
- resp. další informace vztahujících se k licencím.

Pro zdokumentování jasného původu požaduje zadavatel poskytnout dokumentaci obsahující označení prvního nabyvatele softwaru a také číslo smlouvy, pod kterou byl software pořízen, úplný řetězec vlastníků softwaru, potvrzení o odinstalaci od každého z předchozích vlastníků.

Na roveň výše uvedeným požadavkům licencí zadavatel dále připouští dodávku licencí typu OIM k dodávaným serverům, kterou dodavatel prokáže jako příslušenství nabízených serverů.

Jsou požadovány licence pro užití On-Premise.

Zdůvodnění požadavku na kompatibilitu

Zadavatel provozuje své technologické prostředí postavené na platformě OS Windows a MS SQL server. Na této platformě je pak provozována majorita agendových informačních systémů zadavatele, které slouží k zajištění výkonu jeho veřejné správy a dále k zajištění interních činnosti a agend. Na této platformě jsou rovněž provozována adresářové služby a řízení uživatelských účtů a práv v nich. Z těchto důvodů je požadována kompatibilita s tímto technologickým prostředím a jako definice požadavku je uveden konkrétní produktový název.

5 Datové úložiště s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Architektura	Modulární, minimálně dvou řadičové all flash diskové pole active-active designu založené na NVMe architektuře.
	Řešení je koncipováno jako HW, SW a FW od jednoho výrobce.
Výkonnost	Škálování výkonnosti je možné nativním přidáváním dalších řadičů minimálně do osmi řadičové konfigurace a škálování kapacit pomocí expanzních jednotek.
	Škálování řadičů ani expanzních jednotek není povoleno řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů.
Rozšiřitelnost, podporované disky a moduly	Celková velikost cache/RAM v jednom řadiči je minimálně 128 GB.
	Celková nativní rozšiřitelnost je minimálně 30 disků.
	Podpora 2,5” nebo 3,5” disků výhradně technologie SSD/flash a to současně: • podpora SCM (Storage Class Memory), • enterprise úrovně tzn. minimálně eMLC, 3D TLC, SLC nebo eSLC nebo enterprise flash modulů s hodnotou DWPD 2 a vyšší, • SSD s hodnotou DWPD minimálně 1, • všechny požadované typy SSD musí být NVMe architektury, • řešení musí umožňovat nasazení redukce dat v reálném čase tak, aby nedošlo k žádnému ovlivnění výkonu jednotlivých řadičů, tzn. je požadována separátní HW technologie, která je nezávislá na výpočetním výkonu jednotlivých řadičů a zajišťuje maximálně efektivní redukci dat nezávisle na typu ukládaných dat.
	Podpora minimálně následujících režimů RAID - 1, 5, 6, 10 nebo minimálně DRAID 1, 5, 6.
Minimální požadovaná hrubá kapacita a ochrana dat	Tier 0: minimálně 150 TB hrubé kapacity na NVMe bez započtení deduplikace a komprese ve variantě enterprise (DWPD 1 a vyšší, maximální velikost jednoho NVMe modulu je 20 TB).
	Pro tier 0 je požadována ochrana dat minimálně proti výpadku 2 disků/modulů současně.
Požadavky na velikost řešení	Provedení RACK (šíře 19”, výška max.1U).

Konektivita k hostitelským serverům (front-end)	Diskové pole obsahuje připojení diskového pole blokovým přístupem pomocí 32Gbit FC. Jsou požadovány osazené min. 4 porty 32Gb FC na řadič (včetně modulů pro připojení k SAN přepínačům, které jsou rovněž součástí této specifikace. Je požadována možnost osazení minimálně 8x 32Gbit FC portů včetně osazených SW SFP převodníky na jedno dvouřadičové diskové pole s možností rozšíření 32Gbit FC portů.
Funkcionality pro efektivní ukládání a správu dat	Vytváření virtuálních logických disků.
	Thin provisioning (včetně detekce a reklamace prázdného prostoru).
	Komprese dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou nabízenou kapacitu včetně patřičného HW akcelerátoru nebo na jednotlivých modulech.
	Deduplikace dat v reálném čase bez nutnosti dedikování dodatečného diskového prostoru pro post-processing pro celou požadovanou kapacitu včetně SW licence.
	Šifrování dat ve standardu minimálně FIPS 140-2 bez nutnosti přítomnosti speciálních pevných disků včetně příslušné licence. Pokud nabízené řešení neumožňuje šifrování dat nad úrovní disků, jsou požadovány SED disky pro celou nabízenou kapacitu, opět minimálně ve standardu FIPS 140-2.
	Inteligentní správa výkonnostních charakteristik (pro minimálně 3 tiery a to včetně SCM) virtualizovaných diskových prostorů (automatická migrace více utilizovaných dat na rychlejší disky nebo SSD/SCM).
	Podpora externí storage virtualizace pro stávající disková pole a možnost dalšího připojení externích diskových polí od různých výrobců min. pro účely migrace. Seznam podporovaných diskových systému musí být veřejně dostupný.
	Podpora nástrojů pro sledování historických dat o vytížení datového úložiště (minimálně počet IOps, latence, propustnost, alokovaná kapacita, využití keší) s granularitou na hosta či LUN s historií minimálně 1 rok (možnost řešit externích SW nástrojem v rámci dodávky).
	Podpora služby VSS.
	VMware VAAI, VVOL podpora, dále je požadován VASA provider přímo ve FW nabízeného diskového pole.
Podpora operačních systémů a hypervizorů	VMware 7 a vyšší včetně VAAI a VASA integrací.
	Windows server 2019 a vyšší.
Typ přístupu k datům	Blokový.
Bezpečnost	Ochrana proti ransomware útokům nativní vlastnost nabízeného pole v rámci jeho funkcionalit – řešení z aplikační vrstvy pomocí aplikací třetích stran není přípustné. Řešení musí být pro tento účel jasně popsané a určené, např. ochrana LUNu pouze nastavení do read-only modu není dostatečná pro splnění tohoto požadavku.
Funkce synchronizace	Licence musí být součástí nabídky a musí být na neomezenou kapacitu, počet disků, expanzích jednotek atd.
	Zrcadlení virtuálního disku tzn. ochrana virtualizovaných dat v režimu RAID1 (s možností zdvojení dat virtuálního disku i na dvě pole).
	Možnost vytváření snapshotů (CoW a RoW) a klonů v následujících režimech: • Snapshot se po určité době může automaticky stát klonem. • Inkrementální snapshoty, tzn. kopírují se jen rozdílová data mezi dvěma okamžiky iniciace klonu. • Reverzní snapshoty – lze provést zpětné přesunutí dat z klonu do původního originálního Volume. • Lze udržovat až 4 inkrementálně pořizované klony z jednoho originálu (s možností reverzních snapshotů).
	Interní/externí zrcadlení logického (virtuálního) disku z jednoho zdroje do dvou cílů pro zvýšení dostupnosti v případě výpadku jednoho cíle.
Zajištění kontinuální dostupnosti dat (DR a HA řešení)	Licence musí být součástí nabídky a musí být na neomezenou kapacitu, počet disků, expanzích jednotek atd.
	Upgrade software a hardware u řadičů je proveditelné za chodu a bez ztráty přístupu hostitelských serverů k datům.
	Jednotlivá disková kapacita je možné spojit do clusteru, který umožňuje vytvoření jednoho funkčního celku, zrcadlení dat mezi jednotlivými poli apod.
	Vytvoření HA řešení s automatickým failover bez dalších vícenákladů, které je navíc nezávislé na OS nebo virtualizační platformě včetně příslušných licencí.
	Podpora replikace do třetí lokality.
	SW pro redundantní datové cesty v ceně řešení.
	Nabízené řešení musí být plně kompatibilní s VMware Metro Storage Cluster funkcionalitou, tzn. musí být dohledatelné v matici kompatibility na stránkách VMware.
Migrace dat	Transparentní migrace (tzn. možnost zdarma migrovat data ze stávajících diskových polí na nová disková úložiště) s možností rozšíření o synchronní a asynchronní zrcadlení logických (virtuálních) disků v případě více lokalit.

	Bezvýpadková migrace – řešení musí umožňovat migraci dat bez jakéhokoliv přerušení, tzn. aplikace a jejich OS nezaznamenají žádnou nedostupnost dat (LUNů).
Počet hostitelských serverů připojovaných k diskovému poli	Řešení obsahuje licence na neomezený počet připojení hostitelských serverů.
Správa diskového pole a další dostupné funkcionality	SW pro plnohodnotnou správu diskového pole a diskových subsystémů, možnost ovládání přes CLI, GUI (ze std. web browseru).
	Remote Service (call home) v ceně řešení.
	Příkazy prováděné v GUI jsou uchovávány v tzv. "AuditLogu" v podobě standardních CLI příkazů, které lze později snadno zkopírovat a aplikovat při programování uživatelských skriptů např. pro podporu automatizace zálohování atd.
Příslušenství	Součástí dodávky je veškerá potřebná kabeláž pro plné zapojení všech portů do instalovaného prostředí a potřebná napájecí kabeláž kompatibilní s napájecími lištami v RACK skříních.
Požadavky zadavatele na implementaci	Instalace diskového pole v určeném místě zadavatele a propojení s dodávanými servery.
	Instalace posledního stabilního firmware.
	Konfigurace diskového prostoru – nastavení ochrany dat a publikace kapacity směrem k hostům.
	Konfigurace služby call-home.
	Konfigurace vytváření a retence snapshotů na diskovém poli, které jsou odolné pro definovanou dobu proti smazání či modifikaci.
Záruka, záruční servis a podpora	Součástí ceny je záruka a záruční servis v délce trvání min. 36 měsíců zahrnující: • servis v místě instalace, • garantovaná doba vyřešení do 24 hodin od nahlášení poruchy, • SW podporu, která umožňuje např. přístup k novým verzím FW, opravným patchům atd.
	Servisní podpora výrobce bude poskytována v českém jazyce.

6 SAN přepínače

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Konstrukční provedení	Provedení určené k montáži do RACK 19”, ve velikosti 1 U.
Výkonové požadavky	Přepínače musí umožnit duplexní výkon přepínaní při zatížení všech osazených portů plnou rychlostí.
Připojení	Minimální možný počet FC32 portů v rámci switche: 32. Osazené a licencované porty (včetně osazení moduly): • 7x FC32 multi-mode • 1x FC32 single-mode – 10 km • 1x 1Gb RJ-45 OOB Management
Napájení	Dva napájecí zdroje 230 V, připojení k PDU pomocí napájecích kabelů s koncovkami C14 nebo C20 nebo CEE 7/7.
Další vlastnosti	Chlazení v rámci zařízení musí být řešeno tak, aby byl současně aktivně zajištěno ofukování (chlazení) FC portů.
Záruka, záruční servis a podpora	3letá záruka a záruční servis v režimu 8x5 s reakcí a zahájením řešení do NBD od nahlášení závady.
	Po celou dobu podpory bude umožněn legální přístup k originálnímu SW výrobce (Embedded software) jako je zejména certifikovaný firmware, ovladače, BIOS a ostatní software pro konfiguraci, management, monitoring, alerting atd. a k jejich posledním aktualizacím.

7 Pásková jednotka s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Základní parametry	Automatická pásková knihovna v provedení RACK (šíře 19”, výška do 3U).
	Redundantní napájení.
	Barevně označené hot-plug vnitřní komponenty.
	Pro přístup ke všem komponentám není nutné nářadí.
	Dodávka včetně instalačních komponent pro RACK.
	Knihovna musí být vybavena robotickým zakládáním páskových médií se čtečkou čárových identifikačních kódů médií.
	Podpora šifrování, včetně případných potřebných licencí.
Počet mechanik	Jedna mechanika pro pásky typu LTO-9. Mechaniky typu SAS.
	Podpora další rozšiřitelnosti počtu mechanik pomocí expanzních modulů.
Počet slotů	Minimálně 40 slotů knihovny na pásková média, včetně případných potřebných licencí.
Příslušenství	50x LTO9 prázdné médium, včetně štítků čárového kódu od č. 1.
	50x LTO9 WORM prázdné médium, včetně štítků čárového kódu od č. 1.
	1x LTO čistící páska, včetně identifikačního čárového kódu.
	1x SAS kabel pro propojení serveru s knihovnou.
Správa knihovny	Dedikované LAN rozhraní managementu.
	Vestavěné management GUI / webserver.
	Pro monitoring instalovaných OS není třeba instalovat do OS agenta (agent-less/free monitoring OS).
	Podpora SNMP a SysLog serveru.
	Podpora notifikace událostí pomocí SNMP, emailů a napojení na SysLog server.
Instalační služby	Instalace páskové knihovny v určeném místě zadavatele a zapojení do stávající sítě LAN.
	Instalace posledního stabilního firmware.
	Připojení k dodávanému zálohovacímu serveru podle této specifikace.
	Konfigurace včetně nastavení v existující zálohovací platformě, která je specifikována v rámci popisu stávajícího stavu kupujícího v této specifikaci.
Záruka a záruční servis	Záruka a záruční servis v délce min. 36 měsíců poskytovaná přímo výrobcem zařízení nebo jeho autorizovaným zastoupením.

8 Deduplikační jednotka včetně příslušenství

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Velikost	Zařízení musí být v provedení RACK (šíře 19”), výška maximálně 2U, výsuvné kolejnice pro instalaci do racku.
Výkon a škálovatelnost	Řešení musí mít minimálně 70 TB využitelné (usable) lokální kapacity (bez redukce dat včetně všech potřebných licencí pro tuto kapacitu, pokud jsou potřeba).

	Řešení musí umožňovat rozšíření alespoň do úrovně 0,5 PB využitelné lokální kapacity bez redukce dat a bez nutnosti výměny jakékoliv dodávané součásti, cloudové uložiště jako rozšíření není uznatelné.
	Propustnost při zálohování dodávaného řešení (skutečný počet disků a dalších komponent) alespoň 7 TB/hodinu.
	Zařízení musí při ukládání dat využívat princip deduplikace.
	Úložiště nesmí vytvářet deduplikační pooly – musí disponovat globální deduplikací bez ohledu na typ dat, přenosový protokol a množství zálohovacích serverů/aplikací, které na něj data ukládají.
	Řešení musí být postaveno na fyzické instalaci operačního systému bez další virtualizace.
Integrace a interoperabilita	Zařízení musí podporovat minimálně následující protokoly: CIFS, NFS, S3 a musí umožnit jejich současné použití.
	Zálohovací řešení musí být univerzální z hlediska podpory datových typů zálohovaných dat, musí podporovat všechny datové typy používané v produkčním prostředí.
	Řešení musí umožnit komprimaci ukládaných deduplikovaných dat.
	Z důvodu využití stávajících technologických prostředků kupujícího musí být řešení plně podporováno pro produkt Veeam Backup Essentials Enterprise, který je kupujícím nasazen jako stávající platforma a užíván pro zálohování. Oficiálně podporovaná řešení jsou popsána zde: https://helpcenter.veeam.com/docs/backup/vsphere/deduplicating_storage_appliances.html?ver=120.
Replikace	Zařízení musí obsahovat potřebné licence pro nativní funkcionalitu replikace dat do dalšího zařízení stejného výrobce, pro případné budoucí rozšíření.
	Řešení musí posílat pouze deduplikovaná zkomprimovaná data.
	Řešení musí podporovat alespoň následující scénáře pro replikaci: 1:1, M:1 a kaskádovou replikaci.
	Řešení musí umožnit funkcionalitu šifrování replikačního toku data-in-flight.
	Řešení musí umožnit kontrolu a správu využití pásma pro přenos dat (QoS).
Další vlastnosti a parametry	Zařízení musí disponovat redundantními hot-swap napájecími zdroji a ventilátory.
	Zařízení musí zajišťovat ochranu dat alespoň na úrovni duální diskové parity.
	Zařízení musí zajišťovat výměnu všech disků za chodu – hot-swap.
	Zařízení musí obsahovat HotSpare disk pro všechny RAID skupiny v rámci zařízení.
	Zařízení musí obsahovat algoritmy pro kontrolu a verifikaci konzistence a čitelnosti uložených dat.
	Zařízení musí umožňovat nastavit ochranu dat proti nechtěnému smazání či modifikaci dat pomocí časových zámků. Po nastavenou dobu lze data číst, ale nelze je přepisovat. Tato funkce nesmí být závislá na zálohovacím software, přenosovém protokolu (CIFS, NFS, S3) či typu dat. To znamená, že tato funkce musí být plně funkční se stávajícím zálohovacím SW, ale také jakýmkoliv jiným. Časové zámky se musí aplikovat uvnitř zařízení, nikoliv pomocí externích nástrojů a zálohovacích SW.
	Zařízení musí mít integrovanou ochranu časové integrity.
Síťová konektivita	Zařízení musí disponovat síťovými kartami 2x1GbE a 2x10Gb SFP+ včetně multimode transceiverů.
Správa a licence	Řešení musí umožnit centrální správu pro všechna dodávaná zařízení prostřednictvím webového rozhraní.
	Řešení musí poskytovat funkcionalitu automatického reportingu, automatický call-home.
	Řešení musí umožnit správu na principu rolí s různými typy oprávnění (Role-based Access Control).

	Řešení musí umožňovat zasílat strukturovaná data provozních a bezpečnostních událostí přes Syslog a SNMP.
	Řešení musí umožnit dvoufaktorové ověřování účtů pro správu díky jednorázovým heslům (Time-based One-Time Password). Pokud je potřeba externí nástroj, musí být součástí nabídky všechny potřebné licence až pro 25 uživatelů včetně potřebného hardware pro zajištění vysoké dostupnosti. Licence musí být perpetuální a instalace v místě kupujícího.
Záruka, záruční servis a podpora	V rámci povýšení verze softwaru dochází zároveň ke změně verze firmware na kompatibilní úroveň pro důležité komponenty – minimálně pro diskový řadič.
	Požadovaná záruka a záruční servis na nabízené řešení je s reakcí 8x5 NBD po dobu 3 let.

9 Intersegmentační firewall s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
HW požadavky	HW appliance (VM appliance ani software řešení není akceptovatelné).
	Podpora režimu vysoké dostupnosti minimálně jako active/active cluster o dvou fyzických zařízeních.
	Provedení do 19“ rozvaděče, výška 1U.
	Duální napájení (redundantní zdroj).
	Minimálně 8x10 GbE SFP+ sítová rozhraní včetně osazení všech portů SM zářičů 10 Gbit.
	Minimálně 4x1 GbE SFP síťová rozhraní včetně osazení alespoň 2x SM zářičů 1 Gbit.
	Minimálně 10x 1 GbE RJ45 síťová rozhraní.
	Sériový konzolový port
Výkonové požadavky	Minimální propustnost firewallu provoz 35 Gbps (měřeno na UDP komunikaci o paketech s velikostí 512 B).
	Počet současně navázaných spojení firewallu min. 10 000 000, počet nových spojení za sekundu min. 350 000.
	Minimální propustnost IPSEC VPN min. 35 Gbps.
	Propustnost SSL VPN min. 2,5 Gbps.
	Propustnost funkce SSL inspekce min. 7 Gbps.
	Propustnost funkce IPS min. 8 Gbps.
	Propustnost funkce NGFW (stavový firewall + IPS, rozpoznávání aplikací na L7) min. 7 Gbps.
	Propustnost funkce klasifikace aplikací na L7 (pro protokol http) min. 25 Gbps.
	Požadovaná latence firewallu (udp provoz) max. 4,5 µs.
	Min. počet současně připojených uživatelů SSL VPN 500.
Funkční požadavky	Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů.
	Bezpečnostní funkce obecně označovaných jako Next Generation firewall.
	Podpora virtualizace na daném HW, vytváření a provozování tzv. virtuálních kontextů – min. 10 virtuálních kontextů v ceně zařízení; každý virtuální kontext musí pracovat izolovaně, možnost propojovat jednotlivé virtuální kontext pomocí interní virtuálních propojů bez nutnosti použití fyzických interface.
	Podpora stavového firewallingu pro IPv4 i IPv6, podpora NAT 64/46.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Možnost nasazení ve všech z následujících režimů (kombinace možné pomocí použití různých režimů pro různé virtuální kontexty): L2 bridge režim (inline), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline), ZTNA proxy.
	Plnohodnotná správa z lokálního management rozhraní (a to i v případě využití nástroje centrální správy, neboť i v takovém případě musí být možné firewall, resp. firewall cluster, plnohodnotně konfigurovat ve chvíli, kdy z jakéhokoli důvodu centrální správa nebude dostupná).
	Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On.
	Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů.
	Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu.
	Funkce QoS, traffic shaping a SD-WAN minimálně v režimu vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek.
	Podpora funkcí VPN brány: • IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran), • SSL VPN pro klientský přístup s tunelovacím režimem vč. klienta pro osobní počítače i mobilní platformy, portálový režim pro bezklientský přístup.
	VPN klient pro neomezený počet přistupujících zařízení součástí nabídky.
	Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3.
	Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků.
	Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče.
	Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 4000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace.
	Možnost definice zakázaných slov pro vyhledávání na internetu.
	Podpora funkce safe search pro populární vyhledavače.
	Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu.
	Podpora kategorizace streamovaných videí a kanálů min. pro platformu Youtube a Vimeo.
	Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace,

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů.
	Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času.
	Funkce ochrany před unikem citlivých dat (data leak prevention), která umí zachytit pokus o odeslaní/upload označeného dokumentu přes internet na základě vodoznaků, popisu regulárním výrazem atp.
	Podpora dvoufaktorové autentizace pomocí HW, mobilních OTP tokenů, SMS a e-mailu.
	Součástí nabídky musí být 100 mobilních tokenů pro systém Android a iOS a plně funkční řešení dvoufaktorového OTP ověřování uživatelů pro administrátory a uživatele VPN.
	Obousměrná integrace (min. ve smyslu sdílení informací o odhalených hrozbách a provozně/telemetrický informací) nabízeného firewallu s dalšími instalovanými bezpečnostní prvky (e-mailová brána, sandbox, nástroj pro sběr a vyhodnocování logů, nástroj pro centrální správu a poptávaného systému řízení přístupu k sítí).
	Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy.
	Podpora ICAP rozhraní pro obousměrnou integraci s externími servery.
	Podpora tunelování provozu pomocí technologie GRE.
	Podpora automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí.
	Analýza a zabezpečení DNS dotazů (ochrana před DNS poisoningem), filtrování DNS dotazů na základě kategorizace.
	Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu.
	Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algoritmů pro rozklad zátěže (round robin, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz.
Záruka, záruční servis a podpora výrobce technologie	Bezplatný nárok na nejnovější firmware a aktualizace požadovaných funkcionalit, pokud jsou zpoplatněny, min. 36 měsíců.
	Technický support výrobce v režimu 24×7, min. 36 měsíců.

10 Logování firewallů

Technologie musí splňovat následující minimální technické požadavky:

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Parametry, vlastnosti a funkční vlastnosti	Plně kompatibilní s firewally dodávanými na základě této specifikace.
	Virtuální appliance pro platformu VMware vSphere a Microsoft Hyper-V.
	Plná podpora pro instalovanou platformu NGFW.
	Podpora pro Syslog kompatibilní zařízení.
	Výkon logování 6 GB / 1 den.
	Kapacita storage pro logy min. 3 TB.
	Podpora minimálně 4 virtuálních interface.
	Real-time prohledávání logovaných dat.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Kromě historických reportů musí umožňovat i přehled aktuální situace v monitorované síti (možnost okamžitě detekovat problémy a reagovat na ně).
	Vyhledávání podle zařízení.
	Uživatelská definice reportů (vzhled, obsah apod.).
	Možnost rozdělení zařízení na oddělené administrativní sekce (každý virtuální kontext firewallu může být v jiném administrativním kontextu centrálního logovacího zařízení).
	Každý administrativní celek musí mít možnost mít vlastního administrátora, který nebude mít přístup do jiných administrativních celků.
	Obousměrná integrace s dodávanými firewally podle této specifikace, tedy data se přenáší jednak z firewallu na logovací a reportovací platformu, ale zároveň je možné přímo v GUI firewallu přistupovat k log údajům na logovací a reportovací platformě.
	Možnost zašifrování spojení mezi firewallem a nástrojem pro logování, který je předmětem plnění podle této specifikace.
	Event Management – upozorňování na důležité informace z logů (e-mailem a snmp trapy, syslog zprávou).
	Automatické generování reportů v daném čase a periodě.
	Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF.
	Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze.
	Podpora REST API.
Podpora	Bezplatný přístup k firmware a jeho aktualizacím po dobu trvání 36 měsíců.

11 Páteřní přepínač s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Základní vlastnosti	Typ zařízení: L3 přepínač.
	Maximální velikost zařízení: 1U.
	Minimálně 24x 1/10 GbE SFP+ portů s volitelným fyzickým rozhraním.
	Minimálně 4x 40/100GbE portů s volitelným fyzickým rozhraním.
	Podpora rozdělení 40GbE portů na 4x10GbE a 100GbE portů na 4x25GbE.
	Podpora originálních transceiverů výrobce: 10GBASE-T SFP+.
	2x interní hot-swap AC napájecí zdroj.
	Redundantní hot-swap ventilátory.
	Minimální přepínací výkon: 1,28 Tbps.
	Minimální paketový buffer: 32 MB.
Stohovací vlastnosti	Podporovaný počet přepínačů ve stohu: 2.
	Kapacita stohovacího propojení: 400 Gbps.
	Stoh podporuje distribuované přepínání paketů.
	Libovolný prvek stohu může být řídícím prvkem (1:1 redundance).

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Seskupení portů IEEE 802.3ad mezi různými prvky stohu (MC-LAG).
	Podpora upgrade OS ve stohu bez narušení provozu (ISSU/Live upgrade).
	Podpora automatizace upgrade OS ve stohu bez narušení provozu přes REST API.
Funkce a protokoly	Podpora jumbo rámců včetně velikosti 9198 Byte.
	Podpora linkové agregace IEEE 802.1AX.
	Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4.
	Minimální počet LACP skupin/linek ve skupině: 54/8.
	Podpora LACP Fallback (např. pro PXE boot).
	Minimální počet záznamů v tabulce MAC adres: 147 000.
	Minimální počet záznamů v tabulce ARP: 65 000.
	Protokol pro definici šířených VLAN: MVRP.
	Minimálně 1000 aktivních VLAN podle IEEE 802.1Q.
	Tunelování 802.1Q v 802.1Q.
	VLAN translace - swap 802.1Q tagů na trunk portu.
	Podpora zařazování do VLAN podle standardu 802.1v.
	Private VLAN včetně primary, secondary, isolated a community VLAN.
	IEEE 802.1s - Multiple Spanning Tree a IEEE 802.1w.
	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+).
	Podpora ERPS (ITU G.8032) pro rychlou konvergenci do 100ms v kruhových sítích.
	Detekce protilehlého zařízení pomocí LLDP, včetně LLDP over OoB management port.
	Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní).
	DHCP server a relay pro IPv4 a IPv6 včetně podpory VRF.
	Podpora zapouzdření: GRE over IPv4.
	Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace.
	Podpora NTP server.
	Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subnety.
	Podpora L3 routed port včetně L3 sub-interface - nadřazené L3 rozhraní lze rozdělit.
	Statické směrování IPv4 a IPv6.
	Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3, BGP, MP-BGP.
	Funkce BGP konfederace a route reflector pro IPv4 a IPv6.
	Podpora BGP MD5 autentizace a BGP TTL security.
	Podpora police based routing.
	Podpora VRRPv2 a VRRPv3.
	Podpora route map.
	ECMP včetně možnosti konfigurace rozkládání zátěže podle L3 a L4.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Podpora minimálně 62 virtuálních směrovacích instancí (VRF).
	IGMP v2 a v3, IGMP snooping.
	MLD v1 a v2, MLD snooping.
	Směrování multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM, MSDP.
	Hardware podpora IPv4 a IPv6 ACL.
	DHCP snooping pro IPv4 a IPv6.
	ACL klasifikace na úrovni zdrojová/cílová MAC adresa, zdrojová/cílová IPv4/IPv6 adresa, číslo zdrojového/cílového portu, protokol, TTL hodnota , číslo VLAN.
	HW ochrana proti zahlcení portu (broadcast/multicast/unicast) nastavitelná na kbps a pps.
	IEEE 802.1p – Minimálně 8 front.
	802.1X ověřování včetně více současných uživatelů na port, minimálně 64 uživatelů/port.
	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou).
	Dynamické zařazování do VLAN.
	802.1X s podporou odlišných Preauth VLAN, Fail VLAN, Critical VLAN a Critical voice VLAN.
	802.1X a MAC ověřování pomocí odlišných RADIUS serverů aplikované na různé skupiny portů přepínače.
	Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace.
	Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace.
	Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní).
	IP source guard / dynamic IP lockdown.
	Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC.
	Podpora IPv6 RA Guard, DHCPv6 Guard a IPv6 Destination Guard.
	BPDU guard a Root guard.
	Podpora service insertion včetně technologie VXLAN.
	Podpora static a dynamic VXLAN s využitím BGP-EVPN.
	Podpora VXLAN PBR.
	Podpora Group based policy pro VXLAN (VXLAN GBP).
	Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU.
	Vynucení zadat heslo administrátora a nastavitelná politika komplexity hesla přímo na přepínači.
	Možnost instalace vlastního certifikátu včetně podpory Enrollment over Secure Transport (EST).
	TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting).
	Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem.
	Podpora Radius over TLS (RadSec).
	Podpora RADIUS CoA (RFC3576).
	802.1x autentizace přepínače vůči nadřazenému přepínači s podporou EAP-TLS a EAP-MD5.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	QoS ochrana před zahlcením WRED.
	Podpora Data Center Bridging (PFC 802.1Qbb, ETS 802.1Qaz).
	IP Explicit Congestion Notification (ECN).
	Podpora RoCEv2.
Management	CLI formou 1x console port.
	Bezdrátová sériová konzole pomocí Bluetooth.
	Konfigurace zařízení v člověku čitelné textové formě.
	OoB management formou portu RJ45 s podporou ethernetu.
	USB port pro přenos konfigurace a firmware.
	Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient.
	Dvou-faktorová autentizace pro SSH a WebGUI přihlášení.
	Kryptografické SSH algoritmy: AES256, HMAC-SHA2-256, DH s klíčem 3072bit a vyšší.
	Podpora SNMPv2c a SNMPv3.
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL.
	Lokálně vynucené RBAC na úrovni přepínače.
	Dualní flash image - podpora dvou nezávislých verzí operačního systému.
	Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler).
	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů.
	Podpora SYSLOG over TLS.
	Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby.
	Podpora standardního Linux Shellu (BASH) pro debugging a skriptování.
	Podpora skripování v jazyce Python – lokální interpret jazyka v přepínači.
	Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů).
	Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů - možnost vynášení stavu monitorovaných metrik do grafů atp.
	Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.
	Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní).
	Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události.
	Interní uložiště dat pro sběr provozních dat a pokročilou dignostiku zařízení: min. 30 GB.
	Analýza síťového provozu sFlow podle RFC 3176 pro oba směry ingress a egress.
	Analýza síťového provozu IPFIX.
	Ochrana proti nahrání modifikovaného SW prostřednictvím image signing a secure boot, ověřující autentičnost a integritu OS prostřednictvím TPM chipu.
	SPAN a ERSPAN port mirroring, alespoň 4 různé obousměrné session.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	IP SLA pro měření dostupnosti a zpoždění provozu VoIP - režim responder i probe.
	Podpora integrace s automatizačními nástroji (Ansible, NAPALM).
	Automatizace – podpora read-only a read-write REST API včetně volání CLI příkazů.
	Podpora Cloud management software výrobce zařízení.
	Podpora Zero Touch Provisioning (ZTP).
Příslušenství	Propojovací kabel DAC 100 Gb v délce min. 0,5 m. Požadujeme redundantní propojení stacků páteřních přepínačů mezi lokalitami 2x 100 Gb do vzdálenosti 10 km. Vše potřebné (s výjimkou pasivních vláken mezi budovami) pro propojení musí být součástí nabídky.
Záruka, záruční servis a podpora	Záruka, záruční servis a přístup k aktualizacím software v délce 36 měsíců.

12 Přístupový přepínač s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky:

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Základní vlastnosti	Typ zařízení: L3 přepínač
	Velikost zařízení 1U
	Počet 10/100/1000Mbit/s metalických portů: 48x RJ45
	Počet 10Gbit/s SFP+ nezávislých optických portů s volitelným fyzickým rozhraním: 4xSFP+
	Interní AC napájecí zdroj
	Podpora PoE přes kabely Cat3
	Podpora PoE+ dle standardu 802.3at
	Dostupný výkon pro PoE+ napájení 370 W
	Schopnost poskytovat PoE napájení připojeným zařízením i během restartu přepínače
	Podpora Energy Efficient Ethernet (802.3az)
	Minimální přepínací výkon 176 Gbps
	Minimální paketový výkon 130 Mpps
	Minimální paketový buffer: 8 MB
	Maximální hloubka přepínače: 35 cm z důvodu umístění do stávajících podružných RACKů s omezenou hloubkou.
Vlastnosti stohování	Podporovaný počet přepínačů ve stohu: 8
	Kapacita stohovacího propojení: 80 Gbps
	Stoh podporuje distribuované přepínaní paketů
	Podpora stohu na delší vzdálenost minimálně 100m
	Redundance řídícího prvku v rámci stohu
	Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)
	Seskupení portů IEEE 802.3ad mezi různými prvky stohu (MC-LAG)

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Podpora stohování různých typů přepínačů (PoE, Non-PoE, 24port, 48port)
	Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF
Funkce a protokoly	Podpora jumbo rámců včetně velikosti 9198 Byte
	Podpora linkové agregace IEEE 802.1AX
	Konfigurovatelné rozkládání LACP zátěže podle L2, L3 a L4
	Minimální počet LACP skupin/linek ve skupině: 32/8
	Minimální počet záznamů v tabulce MAC adres: 16 000
	Minimální počet záznamů v tabulce ARP: 8 000
	Protokol pro definici šířených VLAN: MVRP
	Minimálně 2000 aktivních VLAN podle IEEE 802.1Q
	Tunelování 802.1Q v 802.1Q
	VLAN translace - swap 802.1Q tagů na trunk portu
	Podpora zařazování do VLAN podle standardu 802.1v
	Private VLAN včetně primary, secondary a community VLAN
	Podpora VLAN-group pro rozkládání klientů přes více VLAN ID
	IEEE 802.1s - Multiple Spanning Tree a IEEE 802.1w
	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)
	Detekce protilehlého zařízení pomocí LLDP, včetně LLDP over OoB management port
	Podpora LLDP-MED
	Detekce jednosměrnosti optické linky (např. UDLD nebo ekvivalentní)
	DHCP server a relay pro IPv4 a IPv6
	Podpora NTPv4 pro IPv4 a IPv6 včetně VRF a MD5 autentizace
	Funkce mDNS brány pro distribuci a filtraci multicast služeb napříč IP subnety
	Podpora L3 routed port
	Statické směrování IPv4 a IPv6
	Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000
	Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000
	Dynamické směrování: RIP, RIPng, OSPFv2 včetně HMAC-SHA-384, OSPFv3
	Podpora police based routing
	Podpora VRRPv2 a VRRPv3
	Podpora route map
	ECMP včetně možnosti konfigurace rozkládání zátěže podle L3 a L4
	IGMP v2 a v3, IGMP snooping
	MLD v1 a v2, MLD snooping
	Směrování multicast: PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM, IPv6 PIM-SSM

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Hardware podpora IPv4 a IPv6 ACL včetně podpory object group pro IP adresy a porty
	ACL definice na základě skupiny fyzických portů
	IN a OUT ACL aplikovatelný na interface, LAG, VLAN
	DHCP snooping pro IPv4 a IPv6
	HW ochrana proti zahlcení portu (broadcast/multicast/unicast) nastavitelná na kbps a pps
	IEEE 802.1p – Minimálně 8 front
	802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port
	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)
	Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675
	802.1X s podporou odlišných Preauth VLAN, Fail VLAN, Critical VLAN a Critical voice VLAN
	Uživatelské role definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely
	Uživatelské role definované lokálně v přepínači, jejich aplikace dle výsledku autorizace
	Uživatelské role dynamicky stahovatelné z RADIUS, jejich aplikace dle výsledku autorizace
	Tunelování uživatelského provozu do L2 GRE tunelů – schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů
	Přiřazení koncového zařízení do tunelu na základě výsledku autorizace
	Podpora bezpečného transportu Dynamic ACL během 802.1X, např. pomocí SSL
	Podpora IPv6 RA Guard, DHCPv6 Guard a IPv6 Destination Guard
	IP source guard / dynamic IP lockdown
	Ochrana ARP protokolu (Dynamic ARP protection nebo funkčně ekvivalentní)
	Port security - omezení počtu MAC adres na port, statické MAC, sticky MAC
	BPDU guard a Root guard
	Podpora service insertion včetně technologie VXLAN
	Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU
	Vynucení zadat heslo administrátora a nastavitelná politika komplexity hesla přímo na přepínači
	Možnost instalace vlastního certifikátu včetně podpory Enrollment over Secure Transport (EST)
	TACACS+ a RADIUS klient pro AAA (autentizace, autorizace, accounting)
	Aktivní monitoring dostupnosti RADIUS a TACACS+ přednastaveným jménem a heslem
	Podpora Radius over TLS (RadSec)
	Podpora RADIUS CoA (RFC3576)
	802.1x autentizace přepínače vůči nadřazenému přepínači s podporou EAP-TLS a EAP-MD5
Management	CLI formou 1x console port
	Bezdrátová sériová konzole pomocí Bluetooth
	Konfigurace zařízení v člověku čitelné textové formě

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	OoB management formou portu RJ45 s podporou ethernetu
	USB port pro přenos konfigurace a firmware
	Podpora IPv4 a IPv6 management: SSHv2 server, HTTPS server, SFTP a SCP klient
	Podpora RSA s délkou klíče minimálně 4096 bitů
	Podpora SNMPv2c a SNMPv3
	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL
	Lokálně vynucené RBAC na úrovni přepínače
	Duální flash image – podpora dvou nezávislých verzí operačního systému
	Konfigurační změny pomocí naplánovaných pracovních úloh (Job scheduler)
	TCP a UDP SYSLOG pro IPv4 a IPv6 s možností logováni do více SYSLOG serverů
	Podpora automatických i manuálních snapshotů systému a možnost automatického obnovení předchozí konfigurace v případě konfigurační chyby
	Podpora standardního Linux Shellu (BASH) pro debugging a skriptování
	Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači
	Možnost vytváření vlastních diagnostických a korelačních skriptů a jejich grafických interpretací v jazyce Python (korelace libovolných událostí a hodnot v podobě grafů)
	Grafické rozhraní pro vynášení výsledků monitorování a analytických skriptů – možnost vynášení stavu monitorovaných metrik do grafů atp.
	Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase
	Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)
	Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události
	Interní úložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení: min. 15 GB
	Analýza síťového provozu sFlow podle RFC 3176 pro oba směry ingress a egress
	Ochrana proti nahrání modifikovaného SW prostřednictvím image signing a secure boot, ověřující autentičnost a integritu OS prostřednictvím TPM chipu
	SPAN a ERSPAN port mirroring, alespoň 4 různé obousměrné session
	IP SLA pro měření dostupnosti a zpoždění provozu VoIP – režim responder i probe
	Podpora integrace s automatizačními nástroji (Ansible, NAPALM)
	Automatizace – podpora read-only a read-write REST API včetně volání CLI příkazů
	Podpora Cloud i On-Premise management software výrobce zařízení
	Podpora Zero Touch Provisioning (ZTP)
Příslušenství	Požadujeme redundantní propojení do páteřních přepínačů v rámci lokality min. 2x 10 Gb. Vše potřebné (s výjimkou pasivních vláken mezi budovami a racky) pro propojení musí být součástí nabídky
Záruka, záruční servis a podpora	Záruka, záruční servis a přístup k aktualizacím software v délce 36 měsíců

13 Přístupový Wi-Fi bod (AP) typ 1 s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Základní vlastnosti	Třída zařízení: indoor přístupový bod
	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 multigigabit 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 30 W 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 2,4 GHz a 5 GHz
	MIMO a počet nezávislých streamů na 2,4GHz rádio: 2x2:2
	MIMO a počet nezávislých streamů na 5GHz rádio: 4x4:4
	Podpora šířky kanálu 160 MHz
	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
	Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 574 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

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	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 2,4 GHz a 5 GHz
	Hardware filtry pro filtraci intermodulačního rušení pocházejícího 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
	Volitelně možnost spravovat AP cloud management nástrojem
	CLI formou serial konsole port a serial over bluetooth
	SSHv2, SNMPv2c a SNMPv3
	AP podporuje zero touch provisioning pomocí externího management SW
	Bluetooth 5.0 Low Energy (BLE) rádio
	Zigbee 802.15.4 rádio
	Podpora režimu SLEEP s max. spotřebou energie do 6W
	Součástí AP je příslušenství pro montáž na zeď nebo strop
Požadavky na implementaci	Fyzická instalace bezdrátových přístupových prvků. Kabeláž do místa instalace je zajištěna ze strany kupujícího
	Zapojení bezdrátových přístupových prvků do sítě a napojení na budované služby včetně 802.1x

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Aktualizace firmware
	Zabezpečení přístupu do managementu AP
	Konfigurace ověřování přístupu do sítě
Záruka a záruční servis	Záruka a záruční servis garantovaný výrobcem zařízení nebo jeho autorizovaným zastoupením s opravou zařízení do 10 dnů v sídle kupujícího po dobu 36 měsíců

14 Přístupový Wi-Fi bod (AP) typ 2 s příslušenstvím

Každý jeden kus zařízení musí splňovat následující minimální technické požadavky.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Základní vlastnosti	Třída zařízení: indoor přístupový bod
	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: 1x 100/1000 Mbit/s RJ45
	Podpora standardů IEEE 802.3af (PoE) a IEEE 802.3at (PoE+)
	Podpora standardního PoE 15,4W bez nutnosti redukce výkonu 5GHz 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
	MIMO a počet nezávislých streamů na 5GHz rádio: 2x2:2
	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: 1200 Mbps
	Minimální komunikační rychlost na fyzické vrstvě (Max data rate) pro 2.4GHz: 574 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

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	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 2,4 GHz a 5 GHz
	Hardware filtry pro filtraci intermodulačního rušení pocházející 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
	Volitelně možnost spravovat AP cloud management nástrojem
	CLI formou serial konsole port a serial over bluetooth
	SSHv2, SNMPv2c a SNMPv3
	AP podporuje zero touch provisioning pomocí externího management SW
	Bluetooth 5.0 Low Energy (BLE) rádio
	Zigbee 802.15.4 rádio
	Podpora režimu SLEEP s max. spotřebou energie do 6 W

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Součástí AP je příslušenství pro montáž na zeď nebo strop
Požadavky na implementaci	Fyzická instalace bezdrátových přístupových prvků. Kabeláž do místa instalace je zajištěna ze strany kupujícího
	Zapojení bezdrátových přístupových prvků do sítě a napojení na budované služby včetně 802.1x
	Aktualizace firmware.
	Zabezpečení přístupu do managementu AP
	Konfigurace ověřování přístupu do sítě
Záruka, záruční servis a podpora	Záruka a záruční servis garantovaný výrobcem zařízení nebo jeho autorizovaným zastoupením s opravou zařízení do 10 dnů v sídle kupujícího po dobu 36 měsíců

15 Licence SW pro nasazení 802.1X a správu síťových prvků

Technologie musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Požadavky na funkcionalitu	Podpora 802.1X autentizace pro bezdrátové sítě, Ethernet LAN sítě a VPN připojení.
	Forma dodání: 2x virtuální appliance v redundantním clusteru.
	Minimální celková kapacita řešení pro autentizaci unikátních koncových zařízení 1000 v redundantním clusteru.
	Řešení musí poskytovat vysokou dostupnost tak aby v případě výpadku primárního AAA serveru převzal jeho roli sekundární server.
	Cluster musí poskytovat vysokou dostupnost pro všechny funkcionality řešení a zároveň možnost navýšení počtu podporovaných uživatelů přidáním další instance.
	Multivendorová platforma – podpora minimálně 20 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.).

Parametr	Popis minimální úrovně parametru
	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.
	Profiling také za pomoci SPAN portu.
	LAN a WLAN Guest portál. Portál musí podporovat možnost přihlašování přes účty minimálně těchto sociálních sítí – Linkedln, Facebook, Twitter. Portál musí umožňovat bohatou grafickou úpravu včetně možnosti přidávání videí a dalšího dynamického obsahu. Možnost samoobslužné registrace hosta do sítě s SMS, e-mail 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 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.
	Jakékoliv funkční rozšíření systému musí být vždy v rámci stejné virtuální appliance jako je AAA systém.
Podpora výrobce technologie	Nárok na nové verze software a bezpečnostní aktualizace po dobu 36 měsíců.
	Možnost otevírat servisní požadavky přímo u výrobce.

16 Licence webového aplikačního firewallu

Technologie musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní požadavky	Technologie typu virtuální appliance s podporou minimálně VMware a Microsoft Hyper-V.
	Operační systém pro Web Application Firewall (WAF) musí být dodáván formou jediného firmware od jednoho výrobce.
	Podpora minimálně 8 virtuálních interface.
	Podpora minimálně 1 vCPU.
	Možnost škálovatelného navýšení počtu vCPU na základě licence.
	Podpora až 2 TB úložiště pro logování.
	Nativní podpora HTTP/2.
	Integrovaný průvodce/wizzard pro nejčastější typy konfigurací.

Parametr	Popis minimální úrovně parametru
Bezpečnostní funkce	Ochrana před OWASP TOP10.
	Funkce Web application firewallu (dále i jen jako WAF): - validace protokolu http (dle RFC), - podpora funkce strojového učení (machine learning) - (dvoúrovňová detekce anomálií a hrozeb za pomoci databáze vzorků výrobce a za pomoci strojového učení (machine learning), - ochrana před klasickými typy útoků na web aplikace (zejména XSS, SQL injection, Cross site request forgery, session hijacking, cookie poisoning), - signatury pro ochranu před útoky na známé webové aplikace.
	Ochrana před útoky typu brute-force.
	Ochrana před útoky na OS & webserver.
	Ochrana před útoky typu L7 DoS/DDoS.
	Podpora geolokační databáze, automaticky aktualizované výrobcem.
	Podpora reputační DB pro IP adresy.
	Rozpoznání a ochrana před přístupem automatizovaných klientů/nástrojů (zejména skenery, crawlery, skripty).
	Funkce user tracking & scoring (Uživatel je identifikován, jeho chování je následně dlouhodobě sledováno a je mu dynamicky upravována reputace na základě reálného chování. Při překročení hraničních hodnot je provedena předdefinovaná akce).
	Funkce Credential Stuffing (Ochrana před kompromitovanými uživatelskými údaji – uživatelské jméno a heslo je kontrolováno oproti databázi kompromitovaných jmen a hesel. Následně je vykonána akce dle nastavení – upozornění nebo zablokování daného uživatele).
	Pokročilá ochrana před false positive.
	Syntax based detection (signatura popisující útok je kombinována s inteligentní analýzou specifického/nestandardního chování s cílem minimalizovat množství false positives min. u SQL injection).
	Antivirová/antimalware kontrola (kontrola uploadovaných souborů): - AV kontrola integrovaná do WAF appliance (nikoliv jako externí zařízení/služba), - ochrana před škodlivým kódem (zejména malware, ransomware, trojské koně) včetně ochrany před polymorfním kódem, - signaturová databáze udržována výrobcem a automaticky aktualizovaná, - funkce sandbox pro ochranu před pokročilým malware, která bude s WAF plně funkčně integrovaná, musí být součástí plnění.
	Podpora formátů XML a JSON.
	Předdefinované politiky pro nejznámější aplikace (min. pro MS Exchange, MS SharePoint, OWA, WordPress).
	Všechny signatury udržované výrobcem a automaticky aktualizované.
	Podporované autentizační mechanismy: - http basic, - klientský SSL certifikát, - podpora dvoufaktorové autentizace (radius access-challenge response),

Parametr	Popis minimální úrovně parametru
	- LDAP, - Radius, - Kerberos.
	Podpora SSO (single sign on): - http basic, - html form, - Kerberos.
Síťové funkce	Podpora IPv4 i IPv6.
	Požadované algoritmy pro L7 load balancing: - Round Robin, - Weighted Round Robin, - Least Connection, - URI hash, - Host hash, - Domain hash, - Source IP hash.
	Požadované metody pro LB persistence: - Source IP, - http header, - URL parameter, - Insert cookies, - Rewrite cookies, - Persistent cookies, - Session ID (ASP, PHP, JSP, SSL).
	Požadované metody pro kontrolu stavu serverů (healthcheck metody): - ICMP Ping, - TCP, - TCP half open, - TCP SSL, - HTTP, - HTTPS.
	URL rewriting.
	Content routing.
	HTTPS offloading, HTTPS inspekce.
	Komprese HTTP.
	Object caching.

Parametr	Popis minimální úrovně parametru
	Vulnerability scanner.
	Vulnerability scanner integrovaný do WAF appliance (možnost interní bezpečnostní kontroly vlastních web aplikací): - výstup ve formátu PDF, - definice automaticky aktualizované výrobcem.
	Možnost automatického importu výsledků auditu pomocí externích nástrojů a následné automatické tvorby bezpečnostní politiky (tzv. virtual patching): - QRadar, - WebInspect, - Qualys, - Acunetix.
Management	Plnohodnotná správa pomocí grafického rozhraní a CLI.
	Management rozhraní provozované přímo na bezpečnostním prvku (bez nutnosti instalovat samostatný management server).
	Správa pomocí web browseru, bez nutnosti instalovat management aplikaci.
	Podpora SNMP včetně MIB souboru dodávaného výrobcem.
Instalační služby	Vlastní instalace do VM a základní nastavení v reverse proxy mode.
	Nastavení publikace webů, certifikáty, security policy a úvodní konfigurace dle doporučení výrobce.
	Publikace OWA.
	Odladění 3 publikovaných aplikací a řešení false positive, bot detection, machine learning, troubleshooting.
Podpora	Nárok na nejnovější firmware, bezpečnostní aktualizace a update software po dobu 3 let.

17 Licence Antivirového systému

Zadavatel požaduje zabezpečit komplexně všechny koncové body, včetně fyzických PC s OS Windows, Mac a Linux, virtuálních PC (VDI) s OS Windows a Linux, fyzických serverů s OS Windows a Linux, virtuálních serverů s OS Windows a Linux a mobilních zařízení s OS Android a iOS.
Na základě hodnocení rizik zadavatel vylučuje technické a programové prostředky výrobců, kteří jsou předmětem varování NUKIB (Varování před hrozbou v oblasti kybernetické bezpečnosti spočívající v nedodržení smluvních závazků ze strany dodavatelů ICT služeb a produktů s významným vztahem k Ruské federaci ze dne 21.3.2022). Zadavatel na základě provedené analýzy rizik vylučuje i bezpečnostní řešení od firmy Kaspersky.

Technologie musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Základní požadavek	Je požadováno řešení pro komplexní ochranu PC, Linux, Mac, mobilních zařízení, fyzické a virtuální serverové infrastruktury, které musí být spravováno z jedné webové konzole.
Konzole pro centrálu správu řešení	
Požadované funkce	Všechny komponenty řešení musejí být v českém jazyce – včetně konzole správy, klientské aplikace a manuálů

Parametr	Popis minimální úrovně parametru
	Požadujeme, aby konzole pro správu byla nasazena i v cloudu výrobce nebo dodavatele, který se stará o její údržbu a vysokou dostupnost veškerých jejích služeb a funkcí
	Možnost kdykoli migrovat konzoli pro správu do on-premise prostředí bezplatně, bez změny platnosti licence a za vynaložení minimálního času ze strany administrátora řešení
	Konzole pro centrální správu je kompletně multi-tenantní
	Podpora produktů výrobcem nástroje bude poskytována v českém jazyce
Základní vlastnosti	Možnost provádět aktualizace klientů z jiných klientů a tím šetřit šířku přenosového pásma připojení k internetu
	Možnost zobrazovat upozornění v konzoli pro správu a posílání upozornění e-mailem
	Možnost zasílat upozornění napojením na Syslog server
	Možnost využití napojení jakékoli třetí aplikace za pomocí zdokumentované veřejné API, k níž je možné vytvářet klíče přímo z konzole centrální správy bez nutnosti zásahu technické podpory dodavatele či výrobce
Úlohy správy bezpečnosti	Řešení musí umožnit integraci se strukturami Microsoft Active Directory za účelem správy ochrany zařízení v těchto inventářích.
	Řešení musí být schopno odhalit stroje, které nejsou vedeny v Active Directory pomocí Network Discovery
	Filtrování a řazení v inventáři alespoň dle jména hostitele, operačního systému, IP adres, přidělených pravidel a dle času poslední aktivity
	Možnost vzdálené instalace a odinstalace EPP klienta přímo z konzole centrální správy
	Možnost upravit úroveň skenovacích úloh a jejich spouštění a plánování, přímo z konzole centrální správy
	Možnost restartovat server nebo desktop přímo z konzole centrální správy
	Centralizované místo pro záznam všech úloh
	Přiřazení bezpečnostních pravidel pro koncové stanice možné granulárně na každé úrovni struktury inventáře, včetně kořenu a listů stromu (tzn. jakékoli OU – organizační jednotky, případně až přímo konkrétní stanici)
Nastavení úrovně bezpečnosti	Více možností přiřazení pravidel: podle uživatele či skupiny v Active Directory, podle síťové lokality, ve které se zařízení nachází (včetně identifikace podle možné kombinace – inkluze či exkluze - následujících znaků: IP adresa, rozsah IP adres, DNS server, WINS server, výchozí brána, typ sítě, název hostitele, DHCP přípona, zda je možné se připojit ke konkrétnímu hostiteli nebo zda je dostupná konzole centrální správy) či dle OU, ve které se nachází v AD
	Možnost nastavení dědičnosti mezi bezpečnostními pravidly granulárně dle sekcí a subsekcí nastavení bezpečnostních pravidel
Reportování	Možnost nastavení intervalu, ve kterém jsou reporty generovány, možnost vytvořit report okamžitě
	Možnost zasílání vygenerovaných reportů e-mailem
	Možnost stáhnout vygenerované reporty minimálně ve formátech minimálně .pdf a .csv
	Možnost upravení reportů, vybrání cíle (skupina stanic, typ stanic atd.) a časového intervalu, ze kterého je report vytvářen
Karanténa	Vzdálená obnova či smazání souboru v karanténě
	Možnost automaticky přidat soubor do výjimky při obnově z karantény

Parametr	Popis minimální úrovně parametru
Administrátor řešení	Více předdefinovaných rolí: Root, administrátor, reportér 1. Root: spravuje komponenty řešení 2. Administrátor: spravuje bezpečnostní pravidla a inventář koncových zařízení 3. Reportér: spravuje a vytváří reporty
	Podpora 2-faktorového ověření a možnost jeho vynucení (uživatel se nepřihlásí, dokud si 2-FA nenastaví)
	Možnost vynutit změnu hesla uživatele po uplynutí určité doby od jeho poslední změny
	Možnost automatického zablokování uživatelského účtu při opakovaných neúspěšných pokusech o přihlášení
	Detailní možnosti vybrat, jaké služby a jaké typy stanic může uživatel spravovat
Logy (záznamy)	Zaznamenávání uživatelských akcí
	Detailní log pro každou akci
	Komplexní vyhledávání v záznamech
Správa a instalace ochrany	Administrátor může před instalací vybrat, které moduly ochrany mají být nainstalovány
	Instalace může být provedena několika způsoby, alespoň: 1. Stáhnutím instalačního balíčku přímo do pracovní stanice, kde bude nainstalován 2. Instalace vzdáleně přímo z konzole správy 3. Distribuce instalačního balíčku pomocí GPO či SCCM
	Instalace klienta na koncové stanice ve vzdálené lokalitě může být provedena z existujícího, již nainstalovaného, klienta v této vzdálené lokalitě – účelem je optimalizace přenosu po WAN/VPN
	Konzole správy bude reportovat počet chráněných koncových stanic a počet koncových stanic, které chráněné nejsou
	Konzole správy obsahuje upravitelné „widgety“ pro okamžitý přehled o stavu ochrany v organizaci
	Konzole správy obsahuje detailní informace o chráněných strojích: zejména název, IP adresa, operační systém, instalované moduly, aplikovaná pravidla, informace o aktualizacích
	Konzole správy umožňuje získání všech informací potřebných pro řešení potíží s ochranou koncové stanice včetně podrobných logů
	Konzole správy umožňuje změnit nastavení hromadně na všech stanicích najednou či třeba jen pro konkrétní skupinu stanic najednou
	Pro rozdílné skupiny uživatelů lze granulárně nastavit, jaké skupiny zařízení mají právo spravovat
	Možnost vytvářet instalační balíčky pro 32-bit a 64-bit operační systémy, včetně samoinstalačního balíčku, který obsahuje kompletní aplikaci a není nutné pro jeho instalaci přístup k síti
	Instalační balíček umožňuje tzn. „tichou“ instalaci (nevyskočí žádné okno, nevyžaduje žádnou uživatelskou interakci)
	Administrátor bude moci v inventáři správcovské konzole vytvářet skupiny a podskupiny, kam bude moci přesouvat chráněné koncové body
	Možnost spustit Network discovery z kteréhokoli již instalovaného klienta
Vlastnosti a funkce ochrany fyzických koncových bodů (Windows, Mac, Linux)	

Parametr	Popis minimální úrovně parametru
Požadovaná vlastnost	Podpora operačních systémů: Windows 10 (včetně IoT Enteprise), 11 a vyšší Windows Server 2019 a vyšší Windows Server 2019 Core Ubuntu 14.04 LTS a vyšší CentOS 6.0 a vyšší Debian 8.0 a vyšší
	Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (zejména LAN, WAN, sdílené úložiště, přenosná média, pevný disk).
	Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů.
	Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru.
	Aktualizace bezpečnostního obsahu alespoň jednou za hodinu.
	Možnost plné ochrany včetně aktualizace pro koncové body trvale bez přístupu k internetu v rámci LAN/WAN sítě.
	Detekce na základě virových definicí (tzn. signatur).
	Threat Emulation Technologie (v cloud prostředí dodavatele nebo lokálně).
	Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům).
	Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům).
	Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení.
	Detekce 0-day útoků na základě odhalování anomálního chování.
	Detekce s využitím strojového učení.
	Modul behaviorální analýzy pro detekce chování nových typů ransomwaru.
	Aktivní ochrany před útoky hrubou silou na protokol SMB a RDP.
	Dynamická detekce 0-day útoků, botnetových sítí, DDos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení.
	Detekce 0-day bezsouborových útoků.
	Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka).
	Ochrana proti neautorizovanému šifrování s automatickou zálohou dat na nepřístupnou část pevného disku s možností automatické obnovy dat po zastavení útoku. Využití stínová kopie svazku ani jiná řešení statického zálohování nejsou z důvodu možnosti jejich odstranění útočníkem přípustné.
	Možnost varování před rizikovým chováním uživatele (zejména přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích).

Parametr	Popis minimální úrovně parametru
	Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně.
	Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno.
	Schopnost pravidelné automatické detekce bezpečnostně rizikových konfiguračních zranitelností operačního systému koncového bodu pomocí vlastního agenta.
	Schopnost pravidelné automatické detekce zranitelností instalovaného SW vybavení na koncovém bodě pomocí vlastního agenta chyběj včetně detailního CVE (Common Vulnerabilities and Exposures) ke každé takové zranitelnosti.
	Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky.
	Možnost automatické detonace podezřelých souborů v Sandboxu s neomezeným počtem detonací.
	Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace.
	Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu.
	Možnost ručního vložení vzorku do Sandboxu.
	Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení.
	Řešení musí obsahovat funkce EDR / XDR integrované do jedné klientské aplikace spolu s EPP (Endpoint Protection Platform).
	Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy.
	Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
	Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
	Řešení generuje detekce na základě automatizovaného hledání IoCs v syrových datech sbíraných EDR senzorem.
	Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku.
	Řešení umožňuje analýzu vektoru útoku.
	Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování.
	Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR).
	Součástí řešení musí být vestavěná antimalware ochrana poštovního serveru Microsoft EXCHANGE provozovaná „onpremise“ na serverech kupujícího.
	Možnost prověřovat http provoz.
	Možnost prověřovat provoz šifrovaný pomocí SSL.
	Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic.
	Možnost šifrovat obsah pevného disku pro notebooky s platformou Windows.

Parametr	Popis minimální úrovně parametru
	Ochrana agenta před neautorizovanou změnou nastavení, vyřazení z provozu, odinstalací antimalware řešení a kritických nastavení.
	Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3).
	Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů.
	Ochrana proti podvodným a phishingovým webovým stránkám.
	Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID.
	Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci).
	Řešení musí umožňovat vzdálené připojení na konzoli koncové stanice s možností výpisu procesů, registrů a souborů, vytvoření, změnu či výmaz souborů či registrů a ukončení procesu, a to i ve stavu izolace stanice od sítě při použití bezpečnostního řešení.
	Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
	Podpora offline prostředí, technologie EDR/XDR vyhodnocuje a reaguje na události lokálně, nevyžaduje pro svou činnost připojení k internetu.
	Grafické zobrazení událostí, které nastaly na koncové stanici při spuštění objektu/procesu (jaký byl sled událostí příkazů, procesů, které procesy, co spouštěly, s jakými komunikovali IP adresami, doménami a tak dále).
	Přehled všech detekovaných technik/taktik MITRE ATT&CK včetně přímého navázání do zobrazeného kybernetického incidentu a linkem do databáze MITRE.
Patch management	Součástí nástroje musí být v rámci jedné konzole od stejného výrobce vestavěná funkcionalita bezobslužná a vzdálené distribuce patchů.
	Distribuce konkrétní záplaty pro definovanou zranitelnost automaticky.
	Distribuce konkrétní záplaty pro definovanou zranitelnost z konzole na vyžádání administrátorem.
	Řešení musí mít možnost definovat úložiště v lokální síti pro snížení dopadů na konektivitu do internetu.
	Možnost zobrazit stav nainstalovaných / chybějících / nefunkčních záplat na koncovém zařízení.
	Součástí záplaty musí být informace (CVE, BuletinID).
	Záplaty lze nástrojem distribuovat na fyzické a virtuální servery Windows, Golden image, pracovní stanice Windows a aplikace třetích stran.
	Možnost odložení restartu pro záplaty.
	Dostupné záplaty pro platformu Windows, Linux a MAC – desktopy a servery.
	Dostupné záplaty pro aplikaci MS Office.
	Dostupné záplaty minimálně pro aplikace výrobců: Adobe Acrobat, Adobe Reader, Google Chrome, Mozilla Firefox, Zoom client, WinZIP, VMware tools.
Firewall pro platformu windows	Možnost blokovat skenování portů.
	Modul musí být možné volitelně kdykoli instalovat a odinstalovat bez nutnosti restartovat OS.

Parametr	Popis minimální úrovně parametru
	Firewall obsahuje systém IDS (Intrusion Detection System) včetně funkce odhalování neznámých hrozeb.
	Možnost vypnout IDS.
	Možnost nastavit profily známých sítí.
	Možnost blokace Network Discovery kompletně (včetně spojení v LAN) či pouze pro spojení z internetu.
Karanténa	Po každé aktualizaci bezpečnostního obsahu jsou automaticky znovu proskenovány soubory v karanténě.
	Možnost obnovy souboru do originální či do nově zadané lokality.
	Automatické mazání souborů v karanténě starších než zadaná maximální doba stáří (maximum nesmí být kratší než 30 dní).
Kontrola přístupu k internetu	Řešení musí umožnit: • Zablokování přístupu na internet pro specifické stanice / skupiny stanic • Zablokování přístupu ke konkrétním webům pro specifické koncové stanice / skupiny stanic • Zablokování přístupu k internetu v určený čas • Zamezení přístupu k typům webových stránek dle výrobcem spravovaných skupin (zejména násilí a hazard) • Zamezení přístupu ke kontkrétní webové stránce (včetně podpory tzn. „wildcards“ pro možnou inkluzi či exkluzi subdomén)
Ochrana virtualizovaných koncových bodů (Windows, Linux)	
Požadavky na funkcionalitu	Produkt nepotřebuje VMware vShield či NSX, aby poskytl tzn. bezenginové skenování – režim klienta, kdy na klientském VM běží jen lehký klient a veškeré úlohy skenování jsou prováděny jiným, speciálním „skenovacím“ zařízením; takové „skenovací“ zařízení může být virtualizováno, ale bez nutnosti, aby bylo umístěno na tom samém hypervisoru jako chráněné klientské VM. Počet těchto speciálních virtuálních zařízení nesmí být licencí nijak omezen.
	„Skenovací“ zařízení jsou spravována z konzole centrální správy – aktualizace, restart, přiřazení jednotlivých klientů k těmto „skenovacím“ virtuálním zařízením.
	„Skenovací“ zařízení musí být možno provozovat v režimu vysoké dostupnosti a rovnoměrného rozložení zátěže.
	Produkt musí hlásit aktuální stav zabezpečení – VM chráněna/nechráněna, a stav „skenovacího“ zařízení.
	Řešení musí umožňovat optimalizaci datových přenosů mezi VM a „skenovacím“ zařízením pomocí deduplikace skenovacích procesů – tzn. ten samý soubor (dle hashe) nebude skenován na dvou různých VM (za předpokladu, že se mezitím nezměnila verze bezpečnostní klientské aplikace).
	Automatické skenování dat, ke kterým je přistupováno – tzn. otevření souboru, kopírování souboru, přenášení souboru (minimálně pro LAN, WAN, sdílené úložiště, přenosná média, pevný disk).
	Automatické skenování souborů v reálném čase může být nastaveno ke skenování pouze specifických typů souborů.
	Automatické skenování souborů v reálném čase může být omezeno na maximální velikost souboru.
	Aktualizace bezpečnostního obsahu alespoň jednou za hodinu.
	Detekce na základě virových definicí (tzn. signatur).

Parametr	Popis minimální úrovně parametru
	Threat Emulation Technologie (v cloud prostředí výrobce, dodavatele nebo lokálně).
	Pokročilá analýza spouštěných procesů ještě před jejich spuštěním a jejich zablokování v případě vykázání škodlivého chování (včetně ochrany proti 0-day útokům).
	Pokročilá analýza běžících procesů v reálném čase a jejich zablokování v případě detekce škodlivého chování (včetně ochrany proti 0-day útokům).
	Detekce 0-day útoků na základě cloudového i lokálního (100% funkce i v případě výpadku připojení k internetu) strojového učení.
	Detekce 0-day útoků na základě odhalování anomálního chování.
	Dynamická detekce 0-day útoků, botnetových sítí, Ddos a exploit útoků v cloudových službách dodavatele pomocí umělé inteligence a pokročilých algoritmů strojového učení.
	Detekce 0-day bezsouborových útoků.
	Detekce 0-day útoků na úrovni síťového provozu (útoky na RDP, pokusy o zjištění dostupnosti, detekce laterálního pohybu útočníka.)
	Možnost automatického hlídání, zda není koncová stanice špatně nakonfigurována a zda nemá nezáplatované aplikace se známou zranitelností.
	Možnost varování před rizikovým chováním uživatele (zejména přihlašování na nezabezpečených webech, používání stejného hesla na mnoha různých webech, používání stejného hesla v interních a externích aplikacích).
	Uvádění tzn. „Risk score“ uživatelů a koncových stanic umožňující administrátorům určit, kterým stanicím a uživatelům je třeba věnovat pozornost prioritně.
	Rizika jsou dle závažnosti ohodnocena a pokud se pojí s konkrétním CVE, tak je uvedeno.
	Možnost automatické nápravy vybraných rizik, případně uvedení návodu k odstranění rizik, které nelze odstranit automaticky.
	Možnost automatické detonace podezřelých souborů v Sandboxu.
	Možnost nastavení Sandboxu – délka pozorování po detonaci, počet opakování detonací, přístup k internetu během detonace ano/ne.
	Akce automatické nápravy na základě verdiktu po provedené analýze v Sandboxu.
	Možnost ručního vložení vzorku do Sandboxu.
	Sandbox po analýze vygeneruje rozsáhlý report o provedené forenzní analýze, včetně: části srozumitelné pro laiky, podrobného shrnutí dění v systému pro experty, časové osy spouštěných procesů a prováděných systémových změn, seznamu a geolokační analýzu síťových připojení, přehledu všech vytvářených, měněných a mazaných souborů a snímky obrazovky případných chybových hlášení.
	Řešení musí obsahovat funkce EDR integrované do jedné klientské aplikace spolu s EPP.
	Řešení musí podporovat možnost izolace infikované koncové stanice. Myšleno tak, že koncová stanice se naprosto odpojí od sítě a bude komunikovat pouze s konzolí centrální správy.
	Řešení musí být schopno logování systémové, procesové a síťové aktivity v době zachyceného incidentu pro další investigaci.
	Řešení umožnuje analýzu síťové komunikace, a na základě analýzy detekuje případné incidenty.
	Řešení u vytvořených incidentů generuje tzv. full execution tree model a časovou osu útoku.
	Řešení umožňuje analýzu vektoru útoku.

Parametr	Popis minimální úrovně parametru
	Řešení umožňuje logování síťových aktivit v době zachyceného incidentu za účelem dalšího prověřování.
	Možnost prověřovat http provoz.
	Možnost prověřovat provoz šifrovaný pomocí SSL.
	Možnost nastavení hesla pro odinstalování EPP klientské aplikace z koncových stanic.
	Modul pro ochranu mailboxů lokálně provozované Microsoft Exchange proti malwaru, spamu a phishingovým útokům.
	Automatické skenování emailů na úrovni pracovní stanice, nehledě na použitém emailovém klientu, obojí pro odchozí (SMTP) a příchozí emaily (POP3).
	Možnost skenovat archivy, možnost nastavení maximální hloubky skenovaných archivů a maximální velikosti skenovaných archivů.
	Ochrana proti podvodným a phishingovým webovým stránkám.
	Detekce používaných zařízení (device) na koncové stanici, možnost blokování zařízení dle typu, možnost povolit pouze konkrétní zařízení dle Device ID.
	Řešení umožňuje tzn. Threat Hunting (hledání IoC v datech sbíraných z EDR).
	Řešení umožňuje ukládat data o bezpečnostních incidentech až 90 dní.
	Všechny vrstvy ochrany implementovány do jedné aplikace (tzn. není nutnost instalovat více než jednu aplikaci).
Rozšířená funkce XDR	
Sonda XDR pro analýzu Microsoft Active Directory	Rozšiřující modul pro XDR – Sonda pro analýzu OnPremise Active Directory.
	Rozšiřující modul pro XDR – Provádí monitorování a zpracování informací o uživatelích z OnPremise Microsoft Active Directory.
	Rozšiřující modul pro XDR – analyzuje a doplňuje incidenty bezpečnostního řešení o informace získané z Microsoft Active Directory.
	Rozšiřující modul pro XDR – sonda pro MS Active Directory musí auditovat bezpečnostní politiky v AD, minimálně Account Logon, Account Management, Object Access, Policy Change a Privilege Use.
	Rozšiřující modul pro XDR – Sonda pro analýzu Microsoft Active Directory musí být plně integrována do řešení ochrany koncového bodu.
	Rozšiřující modul pro XDR – Sonda pro Microsoft Active Directory nesmí zasahovat do chodu MS AD.
	Z konzole bezpečnostního řešení je možno zakázat uživatelský účet nebo vynutit reset hesla v Microsoft AD, který byl použit v rámci bezpečnostního incidentu.

18 Licence software pro zabezpečení elektronické pošty

Technologie musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Obecné požadavky	Ochrana e-mailové komunikace (bezpečná e-mailová brána) fungující jako VM appliance (proprietární operační systém výrobce včetně všech funkcí).
Technické požadavky	Podpora 4 síťových rozhraní v rámci prostředí hypervisoru.
	Podpora VMware ESXi, Microsoft Hyper-V.

Parametr	Popis minimální úrovně parametru
	VM appliance alokuje min. 1 vCPU.
	VM appliance alokuje min. 4 GB paměti.
	VM appliance alokuje min. 1 TB diskového prostoru.
Funkční požadavky	Možnost nasazení v režimu MTA gateway nebo transparentní režim.
	Možnost nasazení v režimu vysoké dostupnosti (včetně sdílení fronty) pro budoucí rozšíření.
	Ochrana proti škodlivému kódu v nevyžádané elektronické poště.
	Podpora víceúrovňové detekce nevyžádané pošty (min. IP, domény, reputační databáze, ověření příjemce, DMARC, SPF, DKIM, proprietární funkce rozpoznávání nevyžádané pošty technikou výrobce, vyhledávání a kategorizace URI/URL, vyhledávání klíčových slov, behaviorální analýza).
	Reakce na detekovaný spam minimálně: - přidání tagu, - přidání hlavičky, - přeposlání e-mailu na jiný SMTP server, - odmítnutí (reject), - zahození (discard), - uložení do karantény, - přepsání adresy příjemce.
	Možnost limitace v rámci SMTP navázané relace (min. počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet e-mailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů e-mailu, možnost manipulace s hlavičkou mailu (odstranění Received hlavičky).
	Antivirová kontrola (antimalware, funkce ochrany proti rychle se šířícím kampaním škodlivého kódu, heuristická funkce detekce škodlivého kódu, detekce dalších variant škodlivého kódu, odstranění aktivního obsahu PDF a kancelářských dokumentů, karanténa, odstranění škodlivých odkazů z emailů.
	Funkce Sandbox musí být součástí řešení.
	Podpora neutralizace dokumentů v příloze v dokumentech MS Office a PDF, při zachování původního typu dokumentu u dokumentů přijatých mimo organizaci.
	Podpora tzv. „Click protection“.
	Podpora IPv4, IPv6.
	Podpora VLAN.
	Plnohodnotná integrace s LOG serverem. Kompatibilita se SIEM.
	Plnohodnotná možnost integrace se síťovým dohledem (podpora SNMP (v2c, v3) včetně dostupnosti MIB souboru dodávaného výrobcem.
Výkonové požadavky	Propustnost min. 25 000 e-mailů za hodinu při průměrné velikosti emailu 100 kB a prováděné kontrole na přítomnost škodlivého kódu a spamu.
	Podpora ochrany minimálně 20 e-mailových domén.
	Licenčně nezávislý model na počtu uživatelů, e-mailových schránek nebo IP adres (pokud jsou tyto funkce licencované, požadujeme dodání licence pro neomezený počet schránek).
Instalační služby	Vlastní instalace do VM a základní nastavení v gateway mode.

Parametr	Popis minimální úrovně parametru
	Provedení dalších nastavení zejména recipient verification, DKIM, DANE, SPF, Sandbox, Auth, karanténa.
	Troubleshooting.
Podpora	Podpora výrobce technologie v délce min. 36 měsíců s reakční dobou na založený incident do konce následujícího pracovního dne (NBD).
	Technická podpora poskytovaná výrobcem v režimu 24x7x365.
	Aktualizace systému a udržování všech požadovaných funkcí dostupné bezplatně min. po dobu podpory. Nárok na nové verze software, update a bezpečnostní aktualizace.

19 HW appliance síťové detekce bezpečnostních hrozeb

Každý jeden kus technologie musí splňovat následující minimální technické požadavky:

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Obecné požadavky	
Systém pro analýzu síťového provozu	Systém složený z hardwarových zařízení musí monitorovat síťovou aktivitu v reálném čase a identifikovat potenciální kybernetické hrozby, bezpečnostní rizika a anomální chování a musí o nich v reálném čase vytvářet upozornění.
	Dodaný systém musí analyzovat síť na základě zrcadleného síťového provozu ze SPAN portů nebo TAPů (nikoliv jen na základě statistických protokolů typu NetFlow) a zároveň bez potřeby nasazovat agenty na koncové stanice nebo další zařízení v síti.
	Systém musí analyzovat obsah datových paketů v reálném čase a detekovat protokol nebo aplikaci na základě obsahu provozu prostřednictvím DPI (Deep Packet Inspection), nikoli pouze čísla portu.
	Dodaný systém musí být schopen analyzovat síť také na základě zpracování statistických protokolů typu NetFlow, IPFIX, NetStream, Cisco NSEL a případně dalších.
	Systém musí být plně funkční v offline prostředí kupujícího bez využití cloudového prostředí pro sběr, ukládání a zpracování dat a veškeré konfigurace a reporting jsou k dispozici přímo v systému.
	Aktualizace systému musí být možné provádět uživatelsky v offline režimu.
Zpracování a ukládání síťových toků	Systém ukládá síťové toky ve formátu, který umožní analýzu síťové komunikace na úrovni jednotlivých toků, včetně dohledání informací o aplikačních transakcích a jejich metadatech z L2 až L7, obsažených v daném síťovém toku.
	Požadované protokoly pro ukládání aplikačních metadat z jednotlivých transakcí jsou: DHCP, DNS, SMB, HTTP, HTTPS, SMTP, SMTPS, POP3, IMAP, SSH, LDAP, LDAPS, KERBEROS, SNMP, CIFS, MSSQL, RDP, SIP, TELNET, FTP, FTP-DATA, TFTP, TFTP-DATA, NFS, ARP, SSL/TLS zapouzdření.
	Je požadováno vysokorychlostní úložiště pro uchování historie datových toků minimálně 1,92 TB složené z SSD nebo NVMe disků.
Analýza aplikačních a systémových logů	Systém musí být schopen sbírat a analyzovat aplikační a systémové logy ve formátu syslog z dohledovaných zařízení a identifikovat nebezpečné nebo potenciálně škodlivé aktivity.
Uživatelské rozhraní	Systém musí poskytovat jednotné grafické uživatelské rozhraní pro veškerou práci uživatelů, včetně všech detekcí, analýzy síťových statistik, nastavení systému, konfiguraci alertů, reportů a dashboardů.
	Systém musí být schopen vytváření profilů a skupin uživatelů pro omezení funkcionality produktu a viditelnosti uložených dat s podporou minimálně:

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	• granulárního nastavení přístupu k analytickým i konfiguračním/administrativním komponentám systému s definovanými úrovněmi přístupu (alespoň read, write, execute), • granulárního nastavení přístupu k datům z různých segmentů sítě organizace s definovanými úrovněmi přístupu (alespoň read, write, execute), • vytváření vlastních filtrů veškerých dat a jejich sdílení mezi uživateli a skupinami uživatelů, • vytváření vlastních uživatelských pohledů, reportů, dashboardů.
Automatické hlášení (alerty) a reporting	Systém musí být schopen upozorňovat uživatele prostřednictvím minimálně emailu a logu o všech identifikovaných událostech a dále o událostech filtrovaných minimálně dle IP a MAC adresy, podsítě, závažnosti události, kategorie události, země, uživatele, síťové služby, čísla portu, provozu do/z internetu.
	Tyto alerty musí být systém schopen dodávat i ve strojově čitelném formátu pro vyžití v nástrojích typu SIEM a musí obsahovat minimálně kompletní informace o detekované události včetně URL odkazu na danou událost v reportovaném období do grafického rozhraní systému.
	Systém musí mít možnost vytváření automatizovaných manažerských reportů o stavu kybernetické bezpečnosti z pohledu zprávy kybernetických incidentů ideálně dle oblastí jejich vzniků (zejména: doména, web, email).
	Je požadováno vytváření automatizovaných reportů v českém jazyce.
Integrace systému	Systém musí poskytovat hotové nástroje umožňující integraci se softwarem třetích stran bez nutnosti použití API systému, a to minimálně: • syslog, CEF a LEEF pro export událostí včetně plné podpory filtrů (exportování pouze požadovaných dat) • přímé url odkazy na libovolnou obrazovku grafického uživatelského rozhraní a filtrovaná zobrazení v grafickém uživatelském rozhraní • export informací o toku ve formátu IPFIX nebo podobném formátu včetně plné podpory filtrů (exportovat lze pouze požadovaná data) včetně aplikačních metadat alespoň pro protokoly HTTP, HTTPS a SMTP • integrace se službami identity uživatelů bez nutnosti konfigurace zasílání logů do systému – minimálně Microsoft Active Directory • integrace s firewall řešením pro automatické a manuální reakce vyvolané systémem • integrace s nástroji pro řízení přístupu k síti pro automatickou a manuální reakci systému.
Požadavky na architekturu nasazení	
Požadavky na zařízení	Pro všechny HW komponenty senzor a kolektor je požadován formát 1U nebo 2U server o velikosti 19“.
	Pro všechny HW komponenty senzor a kolektor je požadován duální zdroj napájení se schopností hot-swap.
	Pro všechny HW komponenty senzor a kolektor je požadováno samostatné síťové rozhraní pro vzdálenou správu serveru v případě výpadku systému typu zejména IPMI, IDRAC, ILO.
	Je požadován 1x HW datový kolektor/sensor o celkové propustnosti minimálně 200Mbps pro 500 monitorovaných IP adres s monitorovacím rozhraním 2x1GbE.
Požadavky na schopnost detekce bezpečnostních událostí	
Monitorování zařízení, segmentů sítě a využívaných síťových služeb	Dodaný systém musí identifikovat všechna zařízení připojená do sítě včetně koncových zařízení, serverů, IoT zařízení apod. Zároveň musí být systém schopen identifikovat změny v síti – minimálně: • změna IP/MAC adresy hosta,

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	• duplicitní IP/MAC adresa, • změna VLAN, • vytvoření nové podsítě, • připojení nového zařízení, • použití nebo vznik nové služby, • nedostupnost dříve dostupné a komunikující služby nebo dříve dostupného a komunikujícího zařízení, • přístup nového zařízení ke službě či zařízení • ověřování platnosti interních certifikátu pro validní TLS šifrování u HTTPS a upozornění před datem jejich vypršení. Systém musí uživateli umožnit pomocí těchto detekčních metod nastavovat bezpečnostní politiky pro různé segmenty sítě a pro různá zařízení a na porušení těchto politik reagovat upozorněním.
Samostatné učení behaviorálních aktivit a detekce anomálií	Systém musí používat matematické metody samostatného učení pro analýzu síťové aktivity, vytvářet a v čase automaticky modifikovat modely chování na základě běžného chování jednotlivých zařízení a na nich provozovaných služeb v rámci celé organizace.
	Systém musí mít schopnost na základě matematického modelu daného zařízení a jeho služeb identifikovat nestandardní síťové chování, a to zejména odchylky od modelu normálního chování pro: • odchylku od modelu pro přenos dat, toků a paketů, • odchylku od modelu pro počet komunikačních partnerů, • odchylku od modelu entropie na komunikačních portech, • odchylku od modelu pro počet síťových toků a využitých síťových služeb, • odchylku od modelu výkonnosti sítě (rychlost přenosu) a aplikací (doba odezvy).
	Samostatné učení je požadováno na všech síťových zařízeních a na nich provozovaných službách (port číslo 0 až 65535 u TCP i UDP) na IPv4 a IPv6 a dalších protokolech L3 a L4 síťové vrstvy.
Identifikace neznámých hrozeb a podezřelých chování	Systém musí být schopen detekovat neznámé hrozby, které nelze identifikovat prostřednictvím detekčních signatur, jako jsou zejména trojské koně a botnety. Zejména musí být identifikovány tyto příznaky potenciálně škodlivého chování: • průzkumné aktivity v síti, • detekce podezřelého strojového chování, které nevytvářejí lidští uživatelé sítě, • detekce repetitivních vzorců chování na síti, • detekce botnetů a ovládání kompromitované stanice, • detekce příznaků těžení kryptoměn, • útoky hrubou silou a enumerace dat, • rozpoznání tunelovaného síťového provozu – alespoň IPv4 prostřednictvím IPv6 a DNS tunely.
Detekce na základě databáze známých hrozeb	Systém musí být schopen identifikovat hrozby a reportovat události na základě • detekční databáze známých hrozeb, tj. malware (zejména trojské koně, viry, červy, rootkity), známých útoků (exploity) a zranitelností, porušení bezpečnostních pravidel a „best practices“ a dalších rizik, • reputační databáze známých škodlivých IP adres, TLS certifikátů, záznamů DNS a hostname, URL adres a hashů souborů.
	Tyto databáze musí být aktualizované minimálně na hodinové bázi. Nesmí se jednat pouze o volně dostupné/open-source databáze, ale musí se jednat o databázi renomovaného vendora nebo poskytovatele těchto služeb, který ji sám bude aktualizovat nebo zajistí její aktualizaci.
	Uživatel musí být schopen importovat vlastní záznamy.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Systém musí využívat tuto detekci pro veškerý monitorovaný provoz (na perimetru i v interní síti mezi všemi segmenty), nikoliv pouze pro omezený segment nebo podmnožinu celkové komunikace.
	Databáze detekčních pravidel (signatur) musí být založena na pokročilých regulárních výrazech pro zpracování řetězců, které dokáží provádět inspekci veškeré síťové komunikace od L2 (Ethernet apod.) po L7. Systém musí detekovat události na základě vysokého počtu signaturních pravidel (minimálně několik desítek tisíc).
	Uživatel musí být schopen prostřednictvím webové aplikace přidávat vlastní detekční pravidla v praktickém a obecně využívaném formátu bez nutnosti znalosti syntaxe a sémantiky pravidel. Příklad syntaxe detekčního pravidla, který musí být možné užít: *alert tcp $HOME_NET any -> any any (msg:"Command Shell Access"; content:"C:\\Users\\Administrator\\Desktop\\hfs2.3b";).*
Analýza šifrované komunikace	Vedle samostatného učení musí systém používat další metody pro analýzu šifrované komunikace, minimálně TLS fingerprinting a s ní spojenou detekci známých hrozeb.
Asistované učení	Je požadován uživatelsky přívětivý proces vytváření pravidel pro zpřesnění detekce a eliminaci falešně pozitivní detekce, a to na základě minimálně následujících parametrů: • IP adresa, • MAC adresa, • hostname, • segment sítě / podsíť, • lokalita – ASN, země, • směr komunikace – určení klienta, nebo serveru, • detekovaná událost – kategorie, název, • použité služby, protokolu, portu, • libovolné kombinaci výše popsaných. Systém musí být schopen eliminovat falešné alarmy i pro události detekované v historii.
Požadavky na zajištění síťové viditelnosti	
Vyhledávání, filtrování a vizualizace dat	Systém musí být schopen okamžitého (v řádu vteřin) vyhledávání a vizualizace pro forenzní analýzu a podporu threat hunting bez zvláštního dotazovacího jazyka.
	Jedná se o možnost okamžitě filtrovat a vyhledávat v plné historii všech uložených dat, tj. bezpečnostních událostí, síťových toků a agregovaných síťových statistikách (tabulky a grafy), a to minimálně: • podle parametrů IP a MAC adresa, hostname, username (identita uživatele), příchozí a odchozí provoz, síťová služba, lokální nebo vzdálená služba (služba z pohledu klient nebo server), číslo portu, VLAN, země, ASN, • prostřednictvím full-textového vyhledávání v datech a vyhledávání na základě definice směru (zdroj, cíl) a logických výrazů and, or, not.
	Systém musí pro vyhledávání poskytovat již předpočítané hodnoty výkonnostních a behaviorálních charakteristik pro každé zařízení v síti a pro všechny na něm provozované služby, bez nutnosti zpracování surových dat ze síťových logů.
	Systém musí být schopen filtrovat a vizualizovat výsledky v grafech, výčtových tabulkách s možností řazení a TOP N statistikách.
	Systém musí být schopen ukládat a následně vyhledávat aplikační metadata (vždy dotaz i odpověď všech transakcí v toku) minimálně z následujících protokolů, které jsou nebo mohou být využívány ve vnitřní síti organizace: FTP, FTP-DATA, TFTP, TFTP-DATA, SSH, Telnet, SMTP, SMTPS, DNS, DHCP, HTTP, HTTPS, NTP, SMB, SNMP, LDAP, NFS, RDP, ARP, MS-SQL, SIP, Kerberos, SSL/TLS.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Metadata jsou v tomto případě chápána jako přenášená aplikační metadata nebo vlastní data servisních protokolů. U protokolu HTTP například http hlavička s metodou, URL, host, user-agent, cookies. V odpovědi pak návratový kód a další http parametry.
	Systém umožnuje provádět uživatelsky jednoduché a okamžité vizualizace síťových prostupů mezi zařízeními a podsítěmi. Využitím uživatelského datového filtru lze vizualizační pohledy libovolně modifikovat.
Kontextuální informace	Systém musí být schopen pro každé zařízení získávat, vizualizovat a v jednom grafickém pohledu zobrazovat kontextuální informace: • jméno uživatele a další jeho parametry z doménového řadiče (MS Active Directory), včetně její historie • hostname zařízení a jeho historie na základě zpracování relevantních dat z DNS a DHCP provozu • IP geolokace • IP reputace, vč. údaje, jestli je IP adresa na blacklistu nebo podezřelá • historie použitých MAC adresa a výrobce zařízení • operační systém a jeho historie na zařízení • uživatelem zadané poznámky a informace k zařízení • automaticky přiřazené značky/tagy zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy • seznam provozovaných a využívaných služeb (klient a server) u daného zařízení a množství na nich přenesených dat • seznam detekovaných bezpečnostních a provozních událostí daného zařízení.
Zaznamenávání, ukládání a zpětná analýza plného provozu	Je požadováno volitelné nahrávání plného síťového provozu (full packet capture) ve formátu PCAP na všech dodaných zařízeních minimálně na základě parametrů: cílová a zdrojová IP/MAC adresa, podsíť, využitý protokol, IPv4 nebo IPv6. Zaznamenávání je možno zapínat automaticky dle detekovaných událostí, nebo uživatelskou aktivací.
	Je požadována schopnost importu vlastního PCAP souboru prostřednictvím webového rozhraní a jeho zpětná analýza všemi detekčními a analytickými prostředky kolektoru.
	Je požadována schopnost zobrazení plného obsahu PCAP souboru v prostředí webového rozhraní aplikace a dále pak automatizovaná analýza surových dat za účelem identifikace provozních nedostatků zachycených pouze v datovém PCAP souboru.
Další požadované oblasti využití	
Monitorování politik kybernetické bezpečnosti	Systém musí umožňovat vytváření komplexních komunikačních a bezpečnostních politik, a to minimálně: • monitorovat definovanou komunikační matici a detekovat, kdy jsou tyto matice porušeny – alespoň jaké zařízení smí komunikovat s jakým zařízením, přes jaký protokol, v jakém čase. • detekce změn v síti – přinejmenším nové komunikační vektory, nová nebo změněná zařízení a podsítě, obcházení perimetru.
	Pro účely monitorování politik kybernetické bezpečnosti musí systém poskytovat uživatelský rámec pro definování pravidel pomocí: • uživatelem definované podsítě na základě rozsahů IP adres • uživatelsky libovolně definovaných skupin zařízení • automaticky přiřazené značky/tagu zařízení, které popisují jejich účel a chování – alespoň server doménového řadiče, webový server, poštovní server, server DNS, server SSH, databázový server, tiskárna, administrátorské zařízení, datové úložiště, aktivní dohledy, skenery zranitelností a technologické systémy.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Management bezpečnostních událostí a incidentů	Systém musí poskytovat funkcionalitu pro reporting bezpečnostních incidentů (prohlášení identifikované události za bezpečnostní incident), včetně: • spolupráci a sdílení informací při analýze identifikovaných bezpečnostních incidentů včetně potřebného workflow mezi jednotlivými uživateli s podporou automatizovaných oznámení o změně stavu události či přiřazení řešitele, • jednoduché sdílení informací o bezpečnostních incidentech, včetně uživatelem zadaných komentářů, • možnost vyhledávání a filtrování nad všemi událostmi z pohledu workflow bezpečnostního incidentů (reportovaná událost, událost v řešení, vyřešená událost, události v řešení daného uživatele apod.), • možnost exportování dat do zejména emailu, csv, pdf, syslogu, • možnost exportu bezpečnostních událostí a incidentů do systémů typu ticket management třetích stran.
Detekce úniku dat	Systém musí být schopen detekovat přenosy citlivých souborů a dat definovaných pomocí jejich názvů, hashů, specifického binárního obsahu (vodoznaku) nebo regulárních výrazů (např. rodné číslo).
	Systém musí být schopen detekovat přenosy citlivých souborů a dat alespoň u následujících protokolů: HTTP, FTP, SMTP, SMB, NFS.
	V rámci historických metadat u HTTP, FTP, SMTP, SMB a NFS je požadováno ukládání informací o všech po síti přenášených souborech alespoň v rozsahu: • název souboru, • velikost souboru, • HASH souboru.
Monitoring výkonu aplikací a sítě	Systém v celé monitorované síti, mezi všemi zařízeními a na všech službách měří a vytváří automaticky (bez nutnosti nastavovat manuálně limitní hodnoty) model normálního chování pro výkonnostní parametry minimálně: • přenosová rychlost sítě, • rychlost odezvy aplikace, • odezva systému z pohledu uživatele.
	Výpočet uvedených výkonnostních parametrů a automatické detekce anomálií na základě odchylky od modelu normálního chování musí být prováděna pro: • všechny porty a služby TCP, • pro všechny kombinace služeb a zařízení.
	Systém musí v celé monitorované síti, mezi všemi zařízeními a na všech službách měřit informace o retransmission paketech, out of order paketech, TTL, QoS a komunikaci blokované firewally.
Monitoring cloudových služeb	Systém musí být schopen monitorovat přístupy zařízení a uživatelů ke cloudovým službám, a to minimálně Google Workspace a Microsoft Office 365, vč. monitoringu operací se soubory, změn oprávnění a nastavení a neúspěšných přístupů.
	Systém musí být schopen tyto informace autonomně a průběžně získávat z aplikačních rozhraní těchto cloudových služeb.
Inventarizace sítě a grafická vizualizace topologie	Systém musí být schopen zobrazit celý inventář monitorované sítě s počtem zařízení v jednotlivých lokalitách, segmentech, nebo podsítích. Včetně detailního přehledu zařízení.
	Systém musí být schopen graficky vykreslit celou topologii sítě, dle zaznamenané komunikace.
	Systém musí být schopen zobrazit inventář jednotlivých lokalit, přehledy zařízení, přehledy výrobců, tagy zřízení, uživatele.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Systém umožňuje všechny inventarizační informace řadit dle různých parametrů.
Záruka, záruční servis a podpora	
Záruka, záruční servis a podpora	Záruka a záruční servis na veškerá dodaná HW zařízení minimálně v rozsahu 3 roky NBD ode dne akceptace (Next Business Day) On-Site.
	Softwarovou produktovou podporu řešení v délce 36 měsíců od podepsání akceptačního protokolu po předáním monitorovacího systému (uvedení řešení do produkčního provozu).

20 Nástroj pro centrální log management

Každý jeden kus technologie musí splňovat následující minimální technické požadavky:

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat	Je požadováno řešení (nebo dále též jako systém) v podobě hardwarové appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Nesmí vyžadovat instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů.
	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware.
	Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřipouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složitě vkládají textové skripty/makra.
	Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně.
	Uživatelsky definované parsery: Systém umožňuje dopsání parserů pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. poddodavatelů) nabízeného systému.
	Uživatelsky definované parsery: Dokumentace dodaná se systémem musí obsahovat přehledný návod na vytváření zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů v jednotném ovládacím grafickém webovém rozhraní.
	Uživatelsky definované parsery: Vytváření a testování parserů nesmí mít vliv na provoz systému. Pro psaní parserů nesmí být použito pouze textové psaní programového kódu, ale systém musí plnohodnotně zajistit vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby.
	Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta.
	Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace, o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: číslo, IP adresa, MAC adresa, URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (zejména součty všech hodnot, průměry, nejmenší/největší hodnota).
	Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí.
	Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
	Možnost sběru událostí minimálně ve formátech RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.
	Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou – administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.
	Systém musí umožňovat konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito pouze textové psaní programového kódu, ale musí umožnit plnohodnotné vizuální programování bez jakékoliv nutnosti užívat textové psaní kódu, které automaticky opravuje uživatele a upozorňuje ho na chyby.
	Systém provádí konsolidaci logů na interním storage logovacího systému.
	Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu.
	Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky.
	Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.
	Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty.
	Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (zejména uživatelské jméno, zdrojová IP, značka/tag).
	Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů nebo obdobné normy plnící minimálně stejnou nebo vyšší úroveň. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit čestným prohlášením.
	Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Od výrobce přednastavené pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.
	Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně pouze SQL jazyk, ale řešení musí umožňovat uživatelsky jednodušší a přívětivější formu.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.
	Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou ve výrobcem přednastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.
	Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být kompletně v českém jazyce. Není přípustná omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran.
	Systém nabízí kapacitní i výkonovou škálovatelnost.
	Požadujeme, aby ze systému bylo možné za běhu vytáhnout libovolný disk, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat výše stanovenou minimální požadovanou kapacitu úložiště.
	Monitoring stavu systému – alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.
	Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (zejména Zabbix, Nagios, MRTG) a umožňoval autorizovaný přístup ke strukturované databázi logů.
	Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní.
	Požadujeme, aby systém umožňoval jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému.
	Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.
	Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.
Minimální HW parametry požadovaného systému	Je požadována hardwarová appliance o velikosti max. 1U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.
	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.
	1 procesor, min. 16 jader, s podporou HyperThreadingu nebo Multi-Threadingu. RAM Min. 64 GB DDR-4 nebo vyšší.
	Minimálně 12 TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.
	Z výkonových důvodů požadujeme, aby v systému byly minimálně 4 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/m a současně nebyly využity všechny šachty na disku a byla tak umožněna budoucí rozšiřitelnost.
	Minimálně 4x 1 Gbit LAN porty + 1x dedikovaný 1 Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému.
	Větráky v systému musí být vyměnitelné za provozu a redundantní.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	2x napájecí zdroje s redundancí napájení 1+1.
	Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače).
	Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (typicky se může jednat o HP iLO, Dell iDRAC apod.).
Výkonnostní a SW parametry systému	Systém funguje formou HW appliance (všechny části systémů je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).
	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému.
	Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce.
	Průměrný trvalý příjem min. 2000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700 byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.
	Špičkový příjem minimálně 4000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700 byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.
	Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 200 GB uložených událostí za den. Integrovaná databáze musí podporovat kompresi ukládaných dat.
	Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (typicky Node-RED, Microsoft VPL, Blockly). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi.
	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy.
	Systém musí podporovat doplňování zpráv o informace z textových prohledávacích tabulek (např. k uživatelskému jménu doplnit z textové prohledávací tabulky informaci o jeho e-mailu, členství v AD skupinách apod.). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes jednotné webové rozhraní.
	Možnost on-line ladění uživatelsky definovaných parserů – při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně.
	V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům značky, označující zejména umístění zařízení, typ zařízení, kritičnost zařízení. Systém obsahuje předdefinované značky, které automaticky přidává k

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	přijímaným zprávám. Příklady značek: konfigurační změna, úspěšné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z Windows, zpráva byla vygenerována firewallem.
	Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.
	Pro budoucí nasazení ve vysoké dostupnosti a výkonnostní rozšíření je vyžadována podpora sestavení ve vysoké dostupnosti – požadujeme podporu minimálně 4 nodů v clusteru. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru.
	Vícenodový cluster se chová i ovládá jako jednotný systém, nutnost nezávislé konfigurace na každé jednotce v clusteru je vyloučena. Vícenodový cluster umožnuje geolokační oddělení a pro komunikaci v rámci clusteru musí využívat definovaný TCP/UDP port pro snadné nastavení prostupy firewallu. Veškerá komunikace v rámci clusteru musí být šifrovaná s vysokým kryptografickým standardem pro bezpečné vytvoření privátní virtuální sítě na síťové vrstvě.
	V případě využití více nodů v clusteru se automaticky zrychluje zpracování vstupních dat a vyhledávání v již uložených datech.
	V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů.
	Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.
	Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.
	Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena.
Alerty	Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.
	Text e-mailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.
	Systém musí obsahovat výrobcem předpřipravené sety / vzory alertů a korelací.
	Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložením příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby.
	Jako výstupní pravidlo alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran.
	V alertech je možné nejen využívat, ale i přiřazovat značky (zejména: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku).
	Systém podporuje funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
Sběr událostí z prostředí produktů společnosti Microsoft	Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému.
	Agent provádí instalaci a podporuje 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.
	Agent sběru z Microsoft podporuje globální i lokální nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. Zejména: *„Zašli pouze logy z adresářů eventview Systém, Security, Sysmon a Terminal Services a zahoď logy s EventId 7036.“*
	Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu.
	Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému, tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy.
	Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše nebo obdobným protokolem stejné nebo vyšší úrovně a musí podporovat ověřování certifikátem.
	Windows agent podporuje sběr nejen ze základních systémových logů (min. Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb a logy rozšířené Sysmonem. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu.
	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K bezpečnostním událostem hodným pozornosti doplňuje značku a popis dle MITRE ATT&CK® matrice a k takto detekovaným procesům a souborům automaticky vytváří hash typu SHA256 nebo vyšší.
Podpora pro sběr událostí z poboček (předpokládané pobočky Městská policie, Knihovna, Městské kulturní centrum)	Systém musí obsahovat centrálně spravované řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.
	Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.
	Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.
	Řešení musí komunikovat po definovaném TCP/UDP portu, aby mohl být snadno nastaven prostup přes firewally a řešena kvalita služby (QoS) pro přenos událostí.
	Řešení musí poskytnout podporu pro sběr událostí na identických UDP i TCP portech jako hlavní dodaný systém.
	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.

Parametr	Minimální parametry (v případě maximálního, nebo fixního parametru, bude toto uvedeno)
	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).
Záruka, záruční servis a podpora	Záruka a záruční servis v délce min. 36 měsíců na HW appliance s opravou v místě instalace serveru a s garantovanou odezvou následující pracovní den od nahlášení případné závady (NBD).
	Systém (SW) musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.
	Podpora software v délce min. 36 měsíců ze strany výrobce na aktualizaci systému a parserů. Podpora musí obsahovat aktualizaci SW minimálně 3x ročně, opravy chyb a telefonickou a e-mailovou podporu s diagnostikou vzdáleným přístupem.

21 Licence software pro řízení přístupových oprávnění administrátorů

Předmětem plnění je dodávka 1 ks řešení Správy privilegovaných účtů (Privilege Identity/Access Management (PIM/PAM)). Řešení bude zajišťovat jednotnou správu a monitoring privilegovaných účtů zadavatele (dále též „kupující“).

Řešení musí být instalováno ve formě virtuálního serveru, který bude provozován na stávající virtualizační infrastruktuře kupujícího.

Kupující požaduje, aby vlastní přihlašovací údaje a klíče k cílovým systémům (operačním systémům, databázím, zařízením apod.) byly uloženy ve vysoce zabezpečené a šifrované databázi systému.

Cíle požadovaného řešení:

- Vyhledání a inventarizace privilegovaných účtů.
- Bezpečná správa hesel a SSH klíčů pro privilegované účty.
- Komplexní správa privilegovaných identit – uživatelů.
- Bezpečný přístup na cílový systém pomocí jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu.
- Centrální kontrolní bod pro izolaci, řízení a sledování všech aktivit správců.
- Monitoring a nahrávání vzdálených relací a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání.
- Kontrola čtyř očí (Dual Control) a oddělení rolí (Segregation of Duties).
- Auditní stopa a personalizace využití sdílených účtů.
- Bezpečný mechanismus pro vyzvedávání hesel a SSH klíčů pro aplikace.

Dodávané řešení musí splňovat následující minimální technické požadavky:

Parametr	Popis minimální úrovně parametru
Požadavky na funkcionalitu	Řešení bude poskytovat správcovský přístup na cílový systém prostřednictvím privilegovaných účtů, ke kterým má uživatel přístup dle bezpečnostní politiky. Účty a systémy, ke kterým nemá práva přístupu, nebudou pro uživatele viditelné.
	Řešení bude umožňovat víceúrovňové schvalování správcovských přístupů k cílovým systémům – přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup k přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém.
	Správcovský přístup na cílový systém bude zprostředkován pomocí jump serveru prostřednictvím zvoleného komunikačního protokolu, aplikace a příslušného privilegovaného účtu tak, aby koncový uživatel neměl přístup k přihlašovacím údajům. Izolace přístupu je možná až na úroveň aplikace (typu webový prohlížeč s konkrétní URL, MMC konzole s vybraným snap-in, konkrétní aplikace jako je např. MS SQL Management Studio, WinSCP, atp.), kdy uživatel nemá možnost přistupovat k jiným službám, aplikacím v rámci dané relace.

Parametr	Popis minimální úrovně parametru
	Po ukončení aplikace se uzavře spojení celé relace. Vzdálené připojení k relaci lze navázat jak přes vlastní GUI dodaného řešení, tak i pomocí standardních protokolů RDP a SSH a standardních klientů typu putty a remote desktop manager. U všech možností připojení ke vzdálené relaci musí být podporováno vynucení silné autentizace (minimálně integrace s LDAP a RADIUS).
	Správcovský přístup prostřednictvím SSH protokolu se bude provádět přes jump server, kde bude uživatel ověřený svými přihlašovacími údaji (je možné spárovat s MS Active Directory) a bude připojený zvoleným privilegovaným účtem na cílový systém bez zadávání hesla a dle bezpečnostní politiky. Pro připojení pomocí SSH Proxy je vyžadována podpora silné autentizace (minimálně integrace s LDAP, RADIUS, či autentizace pomocí SSH klíče).
	Řešení musí umožňovat monitoring a nahrávání celé relace a aktivit privilegovaných účtů ve video formátu s možností kontextového vyhledávání, bez nutnosti instalace agentů na koncový systém. Záznam relace musí být vytvářen kontinuálně, nikoliv formou screenshotů. V záznamech je možné zpětně vyhledávat využitím metadat, které budou mimo jiné minimálně obsahovat: • u RDP relací spuštěné aplikace a události; • u SSH relací jednotlivé příkazy; u Webových aplikací click na jednotlivé odkazy.
	U ostatních typů relací alespoň stisky kláves.
	Pro přehrávání nahrávek není potřeba instalace nástrojů třetích stran (flash, java, codec, atp.) a je dostupné z GUI dodávaného řešení.
	Řešení umožňuje sledovat aktivní relace dalším uživatelem (například auditorem), který v případě potřeby má možnost sledovanou relaci ukončit.
	Systém umožňuje autorizovanému personálu centrálně vyhledávat v nahrávkách podle data pořízení, uživatele a spuštěného příkazu.
	Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS Active Directory a druhým faktorem (minimálně PKI karty, RSA ID, Radius server atp.).
	Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi.
	Řešení zajišťuje audit aktivit uživatelů a správců včetně zajištění vysoké dostupnosti a zabezpečení celého systému (hardening).
	Řešení zaručuje nezpochybnitelnou auditovatelnost jednotlivých operací, možnosti reportování a textové logy. Řešení musí umožňovat nesmazatelnost logů po dobu minimálně 30 dní. Auditní záznamy musí být bezpečně uloženy v zašifrované podobě tak, aby k nim měl přístup pouze oprávněný uživatel.
	Řešení musí podporovat nasazení ve vysoké dostupnosti a vlastní technologické možnosti (nejsou používány nástroje/SW třetích stran) pro zabezpečení High Availability, Disaster Recovery a zálohování tak, aby citlivá data byla stále vysoce zabezpečená a dostupná pouze vlastníkům dat.
	Veškeré komponenty řešení musí splňovat nároky na vysoké zabezpečení a vynucovat tzv. hardening. Úložiště dat, kde jsou uloženy jednotlivé účty, přihlašovací údaje, nahrávky relací a auditní záznamy, je vysoce zabezpečeno a odděleno od ostatních komponent řešení. Databáze dat je součástí řešení a není nutné využívat nástroje třetích stran. Tento požadavek platí pro veškerá data v rámci řešení - i pro HA a DR.
	Žádná z nabízených technologií nesmí být v okamžiku podání nabídky označena výrobcem jako končící = nesmí být označeny jako End of Sale nebo End of Support apod.
	Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze dodávaného softwaru, funkce zařazené na tzv. roadmapu nebudou akceptovány.

Parametr	Popis minimální úrovně parametru
Podpora řízení hesel a bezpečné přístupy pro systémy	Windows 11, 10, Windows Server 2016, 2019, 2022, 2025.
	Linux Red Hat, Debian, Centos,.
	Active Directory, Windows Services, Windows Scheduled Tasks, IIS Application Pool, Windows Registry COM+.
	Virtualizační platformy VMware, HyperV.
	Databáze MS SQL MySQL, PostgreSQL.
	Zařízení Fortinet, Palo Alto, Cisco, Juniper.
	Office 365.
Podpora přihlášení bez nutnosti manuálně vkládat heslo a nahrávání relací pro následující aplikace a protokoly	Protokoly: RDP, SSH, Telnet.
	DB klienti: SQL Manamagement Studio.
	Web GUI: Edge, Chrome.
Architektura	Fully packaged software (obsahuje i OS).
	Podpora pro virtuální prostředí VMWARE nebo Hyper-V.
	Podpora instalace v režimu vysoké dostupnosti.
	Systém dokáže fungovat jako jednotný přístupový bod pro několik instancí v necentralizované infrastruktuře.
	Nástroj musí fungovat jako přístupová proxy.
	Podpora primárního spojeni, minimálně SSH a RDP protokolů mezi privilegovaným účtem a proxy.
	Podpora sekundárního připojení mezi proxy a monitorovaným systémem minimálně prostřednictvím protokolů SSH, RDP, VNC a TELNET.
	Nástroj nesmí vyžadovat žádné instalace software agentů na monitorovaný systém.
	Nástroj musí podporovat integraci s externími uživatelskými databázemi v minimálním rozsahu LDAP/LDAPS/Microsoft Active Directory/RADIUS/KERBEROS/TACACS+.
	Nástroj musí podporovat integraci se SIEM/SYSLOG.
	Nástroj musí podporovat integraci s ICAP pro kontrolu průchozích souborů prostřednictvím antiviru či DLP s možností blokace nežádoucích přenosů.
Správa privilegovaných účtů	Nástroj musí umožnit zaznamenávání administrativních relací.
	Nástroj musí podporovat možnost zhlédnutí záznamu relace prostřednictvím webového rozhraní.
	Nástroj musí zaznamenávat a uchovávat všechny uživatelem zadané příkazy v průběhu SSH a RDP relací.
	Nástroj musí umožnit zaznamenávat a uchovávat názvy všech oken otevřených v průběhu RDP relace.
	Nástroj musí umožnit sběr metadata v průběhu RDP relace alespoň v rozsahu: 1. Změna aktivního okna. 2. Operace s tlačítkem v okně. 3. Volba na radio buttonu či check boxu v okně. 4. Změna obsahu textového pole v okně. 5. Změna rozložení kláves.

Parametr	Popis minimální úrovně parametru
	6. Začátky a ukončení procesů. 7. Manipulace se soubory prostřednictvím clipboardu. 8. Manipulace se soubory prostřednictvím přesměrovaných lokálních diskových jednotek.
	Nástroj musí umožnit nastavení blokace všech, či vybraných TCP spojení zahájených z monitorovaného RDP serveru za účelem navázání neautorizovaných spojení.
	Nástroj musí poskytnout ochranu hesel zadávaných v průběhu RDP relace prostřednictvím detekce vstupu kurzoru do pole pro vyplnění hesla či UAC (User Account Control) okna.
	Nástroj musí umožnit nastavení časových rámců, ve kterých nebude možné navázat spojení (den/čas).
	Nástroj musí umožňovat schvalování přístupu privilegovaného uživatele k určitým monitorovaným systémům.
	Nástroj musí umožňovat ukládání zaznamenaných relací lokálně či na externí úložiště CIFS/NFS.
	Správce nástroje/auditor musí mít možnost pozorovat probíhající relace v reálném čase, včetně možnosti pozorovanou relaci ukončit.
	Při auditu či kontrole proběhlé relace nástroj musí mít možnost zobrazit metadata a videozáznam relace na jedné stránce.
	Systém je spravován pomocí jednotné centrální konzole.
	Systém poskytuje schopnost pracovat se sdílenými účty.
	Nástroj musí poskytovat různé metody autentizace privilegovaných uživatelů na monitorovaných systémech, minimálně: 1. Autentizace privilegovaného uživatele na monitorovaném systému pomocí stejných přihlašovacích údajů, které byly využity pro autentizaci na proxy. 2. Autentizace privilegovaného uživatele na monitorovaném systému pomocí statických a bezpečně uložených přihlašovacích údajů. (např. root, admin, privilegovaný lokální účet). 3. Vyzváním uživatele k opětovnému zadání přihlašovacích údajů k monitorovanému systému, bez jejich zaznamenání.
	Nástroj musí umožňovat schvalování přístupu privilegovaného uživatele k určitým monitorovaným systémům. Schvalování přístupu musí fungovat minimálně v následujícím rozsahu: 1. Privilegovaný uživatel požádá o přístup. 2. Určitý počet PAM administrátorů obdrží žádost o přístupu. 3. Minimální definovaný počet PAM administrátorů schválí žádost. 4. Privilegovaný uživatel získá přístup k monitorovanému systému.
Bezpečnost	Systém musí podporovat shodu se standardy minimálně ISO 27001, HIPAA, SOX, PCI-DSS nebo ekvivalentní stejné nebo vyšší úrovně.
	Bezpečně uložená citlivá data včetně šifrování hesel pomocí AES 256.
	Bezpečné ukládání a správa hesel v certifikovaném trezoru hesel.
	Bezpečná správa a distribuce SSH klíčů.
	Skrývání, odhalování, změna nebo generování cílových hesel.
Licence	Řešení musí být dimenzované pro neomezené množství uživatelů a minimálně 200 cílových systémů.

Parametr	Popis minimální úrovně parametru
	Součástí dodávky musí být také všechny potřebné licence pro operační systémy, databáze a případné další potřebné komponenty systému.
Podpora software	Podpora výrobce v režimu 8x5 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, to vše po dobu 36 měsíců.

22 Požadavky na instalační a implementační práce

Dodané řešení bude sloužit jako vysoce dostupná infrastruktura pro chod agendových IS úřadu a jeho zálohování. Dodávka musí obsahovat kompletní instalaci a implementaci řešení, nad kterým pak bude v režii kupujícího se třetí stranou provedena implementace agendových systémů (virtuální databázové, aplikační a komunikační servery) a konfigurace úloh pro zálohování nově vytvořených virtuálních serverů s agendovými IS.

Implementace dodávaného řešení bude provedena po odsouhlasení zadavatelem a v souladu s „best practice“ a dle doporučení výrobců jednotlivých komponent dodávaného řešení k datu realizace plnění.

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

Dodavatel je povinen zahrnout do nabídky i veškeré další činnosti a prostředky, které jsou nezbytné pro řádné provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, pokud nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.

22.1 Specifikace a rozsah stávajícího vybavení vstupujícího do plnění podle této specifikace

Technologické místnosti

MěÚ provozuje svoje aktiva ve třech lokalitách:

- Lokalita A – MěÚ – Jiřího náměstí 20/I, 290 31 Poděbrady
- Lokalita B – MěÚ – T.G. Masaryka 1130, 290 31 Poděbrady
- Lokalita C – MěÚ – Nám. 5 května 3, 290 31 Poděbrady

Hlavní technologická místnost (serverovna) je umístěna v 1. podlaží v lokalitě A. Místnost je vybavena 2 klimatizačními jednotkami, teplotním čidlem a elektronickým zabezpečovacím systémem. Záložní technologická místnost (serverovna) je umístěna v 9. podlaží v lokalitě B (výtah je do 8. patra a následují schody do 9. podlaží). Místnost je vybavena 2 klimatizačními jednotkami, teplotním čidlem a elektronickým zabezpečovacím systémem. Datové rozvaděče (racky) nejsou vybaveny Rack Management Systémem. Lokalita C je v úrovni sklepa v rámci jednoho podlaží.

Síťové prvky

Síťová infrastruktura je dělena na 2 části. První část vyhrazena pro storage, zahrnuje 5 přepínačů HP 5500-24G-4SFP, které slouží pro propojení diskového pole se servery pro virtualizaci ESX4, ESX5, backup server a k propojení lokalit A a B.

Druhá část (KS01 – LAN MěÚ) je řízena 2 centrálními přepínači HP3500 a je v některých částech segmentována.

Routování zajišťují SW HP 3500 bez filtračních a bezpečnostních politik. Ostatní přístupové SW jsou různého typu, stáří a technických parametrů. Řada SW nepodporuje 802.1x.

Bezdrátová síť je tvořena zastaralými přístupovými body Mikrotik. Z důvodu absence pokročilých bezpečnostních funkcí je tato část sítě izolována a připojena pouze k internetu. V rámci jednání rady města a zastupitelstva města je často požadavek na přístup k lokálním zdrojům, které nyní jsou nedostupné.

Jako hraniční firewall je používán Fortigate 100F.

Serverové a datové prostředí

Hypervisor je do výrobce VMware provozovaný napříč výše uvedenými technologickými místnostmi. Pro realizaci plnění podle této specifikace má již kupující pořízeny licence na pořizované servery pro jejich zapojení do stávajícího clusteru hypervisoru.

Na úrovni operačních systémů pro provoz agendových informačních systémů a samotného doménového prostředí kupující užívá MS Windows server (včetně MS Active Directory), který není možné opustit, protože by to znamenalo nemožnost provozu agendových informačních systémů, které jsou na něm závislé a které kupující pro výkon svých činnosti nezbytně potřebuje.

Jako zálohovací platformu kupující užívá Veeam Backup Essentials Enterprise, kterou má zalicencovánu, provedeny potřebné konfigurace na zálohovaných serverech na úrovni hypervisoru a dále i na úrovni jednotlivých databází a specifických částí provozovaných agendových informačních systémů a jejich konfigurací a dat.
Stávající provozované diskové pole je IBM Flashsystem 5300. U uvedené storage a dvou stávajících serverů je požadováno napojení na nově dodávanou SAN infrastrukturu.
Databázové prostředí
Většina agendových, ekonomických a provozních aplikací a systémů MěÚ využívá platformu MS SQL server.

22.2 Specifikace konkrétních instalačních a implementačních požadavků

V rámci předmětu plnění kupující požaduje provedení min. následujících služeb pro následující oblasti plnění:

- zpracování předimplementační analýzy
- zpracování prováděcí dokumentace
- zajištění projektového vedení realizace předmětu plnění
- dodávku hardware a software
- kompletní implementaci řešení splňující povinné a nabízené parametry technického řešení
- zpracování dokumentace skutečného provedení
- zaškolení administrátorů
- zajištění zkušebního provozu
- provedení akceptačních testů
- předání do ostrého provozu
- zajištění ostatních služeb potřebných pro realizaci projektu

Požadujeme, aby práce mající dopad do fungování IT prostředí kupujícího, byly prováděny výhradně mimo pracovní dobu (tedy byly prováděny v časech 17:00 – 6:00, případně mimo pracovní dny kdykoliv, kontaktní osoby podle smlouvy mohou písemně dohodnout i mimořádný termín, pokud pro to budou na straně kupujícího vhodné podmínky).

Veškerá dokumentace musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standartních formátech (typicky ODT, docx nebo PDF).

Požadavky na technické provedení

Dodané řešení bude sloužit jako Cluster na úrovni hypervisoru a storage pro informační systém města. Instalační a implementační práce musí být minimálně v níže uvedeném rozsahu.

Základní popis prostředí zadavatele:

- Existují dvě datová centra DC1 a DC2.
- Třetí datové centrum pro umístění svědka.
- Konektivita do Internetu je zakončena v datovém centru v lokalitě 1.
- K propojení switchů a Wi-Fi AP bude použita stávající kabeláž kupujícího a nově dodané kabely v rámci tohoto plnění v rámci jednotlivých technických místností a osazovaných prvků.

<u>Dodaná zařízení budou umístěna do třech oddělených datových center a prostředí města:</u>

- DC1 – Lokalita A – MěÚ Poděbrady, Jiřího náměstí 20/I, 290 31 Poděbrady a DC2 – Lokalita B – MěÚ Poděbrady, T.G. Masaryka 1130, 290 31 Poděbrady, prostředí svědka – Nám. 5 května 3, 290 31 Poděbrady
    - technologické komponenty určené pro provoz centralizovaně v serverovnách – servery, datové úložiště, SAN přepínače, LAN páteřní přepínače, pásková mechanika,

deduplikační jednotka, firewally, nástroj pro centrální logování, HW appliance síťové detekce bezpečnostních hrozeb

- Ostatní prostory městského úřadu města Poděbrady
    - Přístupové přepínače
    - Přístupové Wi-Fi body

Konečné umístění jednotlivých technologií bude předmětem upřesnění společně se zástupci kupujícího a bude detailně prodávajícím zpracováno do návrhu předimplementační analýzy, včetně přesného umístění, formy napojení a montáže.

Rozmístění technologií, které nejsou konkrétně uvedeny ve výčtu výše, mezi technologické místnosti upřesní kupující dodavateli (dále též jako „prodávající“) v rámci součinnosti při zpracování předimplementační analýzy.

V rámci přípravných prací prodávající provede:

- návrh a segmentace sítě pro nově nasazované technologie, včetně návrhu adresního plánu (minimálně oddělení jednotlivých typů komunikace do samostatných VLAN); v DC1 kupující již provozuje firewall typu FortiGate 100F, kupující pro tento firewall umožní prodávajícímu přístup k na něm vedeným pravidlům a konfiguracím za účelem možnosti jejich promítnutí do navrhované úpravy sítě a dále bude v rámci plnění po prodávajícím požadovat jejich konfiguraci ve vazbě na nově upravenou segmentaci sítě a nově nastavovaná pravidla v síti; kupující současně požaduje přenesení odpovídajících pravidel firewallů a jejich konfiguraci na jím dodávané řešení firewallu do DC2 v rámci plnění této specifikace; případně je kupující připraven provést export pravidel do standardizovaného formátu pro jeho analýzu a zpracování prodávajícím
- nasazení nové SAN infrastruktury v podobě SAN přepínačů do serveroven a napojení stávajícího a v rámci tohoto plnění dodávaného datového úložiště do SAN infrastruktury a konfigurace služeb pro zajištění vysoké dostupnosti budovaného SAN prostředí jako prostředků pro provozované prostředí
- návrh konvence DNS názvů pro jednotlivá zařízení
- definice parametrů SNMPv3 případně SNMPv2c zabezpečení
- návrh a nasazení oddělené sítě pro správu
- návrh konfigurace svazků datových polí a disků (velikost, replikace, dostupnost)

V rámci instalačních a implementačních prací:

- montáž dodaných zařízení do stávajících datových rozvaděčů
- redundantní zapojení napájení jednotlivých zařízení se zohledněním dostupnosti UPS v serverovnách
- popis všech kabelů na obou koncích (datové i napájecí)
- konfigurace portů pro správu a karet pro vzdálenou správu jednotlivých zařízení a jejich připojení do vyhrazené sítě pro správu
- aktualizace firmware v jednotlivých zařízeních a jejich komponentách na nejnovější doporučené verze
- zabezpečení přístupu ke správě jednotlivých zařízení, konfigurace synchronizace jejich času, konfigurace SNMP parametrů pro možnost vzdáleného dohledu, konfigurace SMTP pro zasílání e-mailové notifikace o stavu zařízení

- vytvoření logického stacku páteřních přepínačů v rámci DC1 a DC2
- konfigurace agregačních skupin přes přepínače v rámci lokality (MC-LAG s LACP) na přepínačích pro propojení přepínačů, připojení serverů a úložišť
- konfigurace VLAN, povolení jen potřebných VLAN na trunk portech
- nastavení všech páteřních přepínačů jako brána pro všechny VLANy směrované na přepínačích
- nasazení Spanning-Tree protokolu (MSTP) na síťových prvcích, root guard, loop protection
- **nasazení protokolu 802.1X na rozhraní sítě včetně systému (řešení) jeho centrální správy a řízení**, tedy zejména na dodávaných přístupových přepínačích a access pointech prostřednictvím RADIUS protokolu s využitím MS Active directory a informacích o uživatelích a zařízeních v organizaci; dodávka dokumentace centrální správy a distribuce pravidel 802.1X pro zabezpečení přístupu do sítě
- redundantní zapojení serverů k přepínačům
- instalace a konfigurace hypervizoru na příslušných serverech v aktuálních verzích
- nasazení a konfigurace clusteru
- instalace a konfigurace datových úložišť, aktualizace na aktuální verze
- na produkčním datovém úložišti vytvoření replikovaných svazků, které budou bez výpadku dostupné i při výpadku jednoho ze serverů
- instalace operačního systému a jeho aktualizací na produkčních serverech, instalace ovladačů a nástrojů pro správu od výrobce serveru
- instalace zálohovacího software na zálohovací server a jeho konfigurace (konfigurace zálohovacích úloh) – ke stávajícím konfiguracím zajistí přístup kupující, který rovněž poskytne údaje k licenci stávajícího software zálohování (uveden výše v popisu stávajícího vybavení)
- kompletní ověření funkčnosti celého řešení
    - vytvoření testovacích virtuálních serverů ve virtualizační infrastruktuře
    - simulovaný výpadek jednoho z páteřních přepínačů
    - odpojení jednoho z propojů mezi páteřními přepínači
    - otestování korektní konfigurace Spanning-Tree protokolu vytvořením smyčky mezi přepínači
    - otestování odstávky/výpadku jednoho produkčního serveru
    - otestování redundantního napájení jednotlivých zařízení střídavým odpojením jednoho z napájecích zdrojů
    - otestování funkčnosti korektního vypnutí jednotlivých serverů při výpadku napájení
    - otestování funkčnosti vypnutí celé nově rozšířené infrastruktury při výpadku napájení a jejího korektního nastartování po obnovení napájení

22.3 Specifické implementační požadavky pro jednotlivé oblasti

Zvýšení zabezpečení komunikační sítě
- analýza stávajícího síťového prostředí a návrh nové architektury LAN, - implementace pořízených technologií, - provedení segmentace sítě – VLAN, adresování, routování, - zavedení DNSSEC, vybudování DNSSEC resolveru pro LAN úřadu,

- návrh a implementace systému 802.1X pro LAN a WiFi včetně definice přístupových politik. Systém 802.1x musí být integrován s adresářovou službou Active Directory,
- implementace portálu pro registraci a řízení přístupů hostů – tzv. captive portál
- zpracování uživatelské dokumentace konfigurace obvyklých zařízení a jejich systémů pro systém 802.1X – PC, notebooky, chytré telefony, tablety, tiskárny – Windows, Linux, MacOS, Android, IOS, embedded systémy periferií. Provedení vzorové migrace a konfigurace všech kategorií koncových zařízení (1 zařízení každé kategorie) do systému s ověřováním 802.1X
- návrh a vybudování vhodné architektury WiFi s více SSID pro zaměstnance, jejich osobní zařízení a veřejnost s vhodným způsobem ověřování a politikami řízení provozu,
- návrh a implementace firewallu včetně vhodné konfigurace UTM (antivir, IPS, aplikační kontrola, URL filtrace dle kategorií, zajištění bezpečné publikace interních zdrojů úřadu, vybudování VPN na bázi webového portálu.
- převzetí komunikačních pravidel ze stávajícího firewallu a jejich implementace do nového firewallu včetně optimalizací využívajících pokročilých vlastností nového řešení. Export pravidel ze stávajícího firewallu zajistí kupující.
- provedení potřebných migrací a konfigurací stávajících systémů – export konfigurací stávajících síťových systémů provede kupující
- návrh a provedení akceptačních testů.

Vytvoření serverového prostředí s vysokou dostupností pro provoz IS

- analýza současného prostředí s ohledem na systémové a kapacitní nároky systém a aplikací
- návrh a rozšíření virtualizační platformy v kontextu nově dodávaných technologií a zvýšení dostupnosti provozovaného prostředí jako celku, a to pro provoz současných a dodaných systémů
- návrh rozšíření stávající platformy aplikační virtualizace včetně nastavení uživatelského prostředí a vhodných politik
- začlenění veškerých dodaných systémů a technologií do zálohovacích plánů organizace (pásková mechanika, deduplikační jednotka)
- provedení potřebných migrací (v rámci plnění nejsou požadovány migrace jednotlivých VM, které jsou již v prostředí hypervisoru provozovány, a když dojde v rámci plnění k rozšíření hypervisoru o nové prostředky, které zajistí zvýšení dostupnosti pro tyto VM v případě výpadku jeho jednotlivých HW komponent)
- provedení potřebných konfigurací souvisejících systémů
- návrh a provedení akceptačních testů

Nasazení systému řízení privilegovaných účtů a zařízení administrátorů

Privilegované účty

- analýza ICT prostředí se zaměřením na vyhledání a inventarizace privilegovaných účtů
- vybudování systému pro správu a řízení privilegovaných účtů včetně napojení monitorovaných systémů a nastavení rotace hesel
- provedení potřebných konfigurací souvisejících systémů
- návrh a provedení akceptačních testů

Zavedení nástroje pro centrální log management IS a KS, jeho uživatelů a administrátorů

Sběr a správa logů

- analýza a detailní identifikace zdrojů dat, jejichž provozně bezpečnostní informace bude nutné, popř. vhodné sbírat. Bude obsahovat i návrh způsobu zpracování získaných informací a vhodných proaktivních i reaktivních akcí
- návrh a vybudování systému centrálního logování pro zaznamenávání činnosti informačního a komunikačního systému, jeho uživatelů a administrátorů
- monitoring a logování NAT (RFC 2663) provozu za účelem dohledatelnosti veřejného provozu k vnitřnímu zařízení (ve spolupráci s firewallem)
- logování přístupu uživatelů do sítě umožňující dohledání vazeb IP adresa – čas – uživatel, a to včetně ošetření v případě sdílených pracovních stanic (aplikační virtualizace) apod.
- monitorování IP datových toků formou exportu provozních informací o přenesených datech v členění minimálně zdrojová/cílová IP adresa, zdrojový/cílový TCP/UDP port (či ICMP typ) dle RFC3954 nebo ekvivalentu (např. netflow) – minimálně na úrovni rozhraní WAN
- provedení souvisejících konfigurací monitorovaných systémů
- návrh a provedení akceptačních testů, musí zahrnovat i testy archivace a obnovy logů

Sběr a vyhodnocení síťových toků

- nasazení a konfigurace HW appliance síťové detekce bezpečnostních hrozeb a její nastavení pro potřeby objednatele na základě doporučených metodik a metrik výrobce technologie a její napojení na centrální logování - analýza komunikačního systému a návrh způsobu sběru a obsahu síťových toků a logovaných událostí - vybudování systému sběru a analýzy síťových toků a souvisejících bezpečnostních událostí - provedení souvisejících konfigurací monitorovaných systémů - ukládání informací (min. o bezpečnostních událostech incidentech do systémů sběru a správy logů) - návrh a provedení akceptačních testů
Nasazení software pro zabezpečení el. pošty
Požadavky obsaženy výše jako součást specifikace technologie.
Webový aplikační firewall
Požadavky obsaženy výše jako součást specifikace technologie.

22.4 Požadavky na předimplementační analýzu

Dodavatel před implementací řešení zpracuje předimplementační analýzu, minimálně pro následující oblasti:

- způsob začlenění nabízeného řešení do stávajícího ICT prostředí
- analýza požadavků na síťovou infrastrukturu
- analýza požadavků na ukládání a zálohování dat, obnovu dat, toky a objemy dat
- požadavky na rekonfigurace stávajících systémů ve vztahu k plánovanému využití
- dopady implementace na dostupnost a funkčnost stávajících služeb
- další podklady relevantní pro návrh řešení
- požadovaná součinnost zadavatele
- návrh opatření k odstranění neshod zjištěných v průběhu analýzy

Výstupem předimplementační analýzy bude písemná zpráva podléhající schválení kupujícím.

22.5 Požadavky na zpracování prováděcí dokumentace

Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude důsledně vycházet z předimplementační analýzy a bude zahrnovat všechny aktivity potřebné pro řádné zajištění implementace předmětu plnění.

Prováděcí dokumentace musí být před zahájením prací písemně schválena kupujícím.

Prováděcí dokumentace musí zohlednit podmínky stávajícího stavu, požadavky cílového stavu a musí obsahovat minimálně tyto části:

- detailní popis cílového stavu včetně popisu funkcionalit jednotlivých HW a SW částí systému
- způsob zajištění koordinace realizace předmětu plnění s běžným provozem
- detailní návrh a popis postupu implementace předmětu plnění
- detailní popis zajištění bezpečnosti informací
- detailní harmonogram projektu včetně uvedení kritických milníků
- návrh designu úložišť a virtuálních serverů a jeho konfigurace
- návrh designu zálohování a jeho konfigurace
- návrh designu síťového řešení a jeho konfigurace
- návrh monitorování řešení monitorovacími nástroji
- vazby na stávající systémy a jejich konfigurace
- návrh akceptačních kritérií a akceptačních testů
- detailní popis navrhovaných školení

Dokumentace skutečného provedení bude před akceptací plnění aktualizována na skutečně provedenou podobu, včetně konečné podoby provedených konfigurací.

22.6 Požadavky na provozní dokumentaci

Provozní dokumentace bude zpracována a předána v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat všechny dodané systémy.

22.7 Požadavky na zajištění projektového řízení

Dodavatel zajistí projektové řízení po celou dobu realizace plnění certifikovaným specialistou. Dodavatel zpracuje a předloží popis metodiky, která bude použita pro projektové řízení, v rámci uzavírání kupní smlouvy na plnění veřejné zakázky.

22.8 Požadavky na zaškolení

Dodavatel zajistí zaškolení zaměstnanců zadavatele – administrátorů – na zařízení a systémy, v rámci tohoto plnění, a to minimálně v rozsahu předávané provozní dokumentace.

- Zaškolení zajistí seznámení specialistů IT kupujícího se všemi podstatnými částmi plnění v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
- Minimální rozsah zaškolení je 8 hodin.
- Zaškolení bude probíhat v sídle kupujícího.
- Předpokládá se účast 2 administrátorů.
- Náklady na zaškolení musí být zahrnuty v nabídkové ceně k položce, ke které se vztahují.

22.9 Požadavky na provedení zkušebního provozu a akceptačních testů

- Dodavatel zajistí pro realizovanou část zkušební provoz v délce minimálně 10 dnů se zajištěním technické podpory specialistů na dodané řešení s možností nahlášení požadavku v pracovní den v době od 8 hod. do 16 hod. a dobou reakce od nahlášení požadavku do 4 hod.
- Dodavatel navrhne způsob a provedení akceptačních testů, který bude podléhat schválení ze strany kupujícího.
- Součástí akceptačních testů musí být minimálně kompletní ověření funkčnosti celého řešení dle této specifikace, a to minimálně v následujícím rozsahu
    - Ověření (otestování) požadovaných funkcí a parametrů.
    - Provedení zátěžových testů a změření výkonových parametrů (rychlost, odezvy aplikací) na testovacím prostředí.
    - Otestování vysoké dostupnost řešení na testovacím prostředí.
    - Provedení zálohy a ukázkové obnovy dat na testovacím prostření.
    - Testovací prostředí pro ověření funkčnosti a schopností nově implementovaných technologií bude navrženo prodávajícím v rámci prováděcí dokumentace a musí respektovat omezení plynoucí z nutnosti zachovat plný provoz stávajících technologií do okamžiku převzetí činností nově nasazenou technologií. Jeho rozsah a forma provedené bude podléhat schválení kupujícím jako součást odsouhlasení prováděcí dokumentace.
- O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol.
- Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace plnění včetně vypořádání všech vad a nedodělků.

22.10 Další požadavky na záruky, záruční servis a další podmínky v rámci záruky

- Nabídne-li dodavatel v rámci svého řešení HW, na něž výrobce standardně (tj. v rámci standardní dodávky a ceny) poskytuje horší záruku, popř. podporu, požaduje kupující zahrnout do nabídky cenu povýšení záruky, popř. podpory na jím požadovanou úroveň.
- Kupující požaduje přístup k aktualizacím software a firmware dodaného HW v kupní ceně minimálně po dobu záruky.
- Veškeré opravy po dobu záruky budou provedeny bez dalších nákladů pro kupujícího.
- Není-li uvedeno u dané položky požadovaného HW jinak, požaduje zadavatel provedení záruční opravy do deseti pracovních dnů.

23 Harmonogram plnění

Kupující požaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro realizaci dodávky. Údaj D značí datum nabytí účinnosti kupní smlouvy. Čísla značí počet kalendářních dnů.

Aktivita	Začátek	Termín splnění
Nabytí účinnosti smlouvy (uveřejnění v registru smluv)	D	D
Zahájení projektu – úvodní projektová schůzka	D	D+7
Předimplementační analýza – zpracování	D+7	D+17
Předimplementační analýza – připomínkové řízení, schválení	D+17	D+24
Prováděcí dokumentace – zpracování	D+24	D+34
Prováděcí dokumentace – připomínkové řízení, schválení	D+34	D+40
Realizace předmětu plnění	D+40	D+80
Školení administrátorů	D+80	D+90
Zkušební provoz	D+90	D+110
Akceptační testy	D+110	D+120
Zahájení ostrého provozu	D+120	-

Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.

Maximální lhůty trvání nesmí dodavatel při tvorbě detailního harmonogramu prodloužit.

Detailní harmonogram plnění uvede dodavatel ve své nabídce.

Dodavatel uvede potřebnou součinnost kupujícího pro splnění harmonogramu plnění ve své nabídce.

Tomáš Ječmínek
Digitally signed by Tomáš Ječmínek
Date: 2025.12.08 11:58:58 +01'00'

Ing. Jaroslav Dvořák
Digitálně podepsal Ing. Jaroslav Dvořák
Datum: 2025.12.08 11:13:43 +01'00'