Technická specifikace

Datové pole

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 128GB • celková nativní rozšiřitelnost je minimálně 700 disků, v případě nasazení více řadičů až čtyřikrát tolik disků. Jak je popsáno výše na řádku výkonnost, nelze toto řešit pomocí externí virtualizace nebo podvěšením dalšího pole a řadičů • 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 tak 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
Minimální požadovaná hrubá kapacita a ochrana dat	• Tier 0: minimálně 115 TB na SSD / Flash ve variantě enterprise (DWPD 2 a vyšší). • 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)	• Je požadováno min. 2 porty 12Gb SAS na každém řadiči
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 je 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) • Microsoft VSS podpora
Podpora operačních systémů a hypervizorů	• Windows server 2019 a vyšší

Typ přístupu k datům	• Blokový
Bezpečnost	• ochrana proti ransomware útokům nativní funkcionalitou 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 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 možnosti 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. • Je požadováno potvrzení od lokálního zastoupení výrobce, že nabízené řešení je určeno pro český (EU) trh a bude servisním střediskem výrobce plně podporováno. Servisní podpora výrobce bude v českém jazyce

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.

Server pro virtualizaci - 3 ks

Typ zařízení	• Server v provedení k instalaci do 19" racku, maximálně 1U. • Barevně označené hot-plug komponenty. • Pro přístup ke všem komponentám není nutné nářadí. • Zásuvné ližiny s managementem kabeláže. • Šasi se zvýšenou odolností, s certifikací trvalého provozu -5 ~ 45°C osazený čelním panelem s filtrem nasávaného vzduchu
Procesor	• CPU uvedený na trh nejdříve ve Q2/2021 • Z licenčních důvodů maximálně 16x Core • Avarage CPU mark min. 35000 v hodnocení na www.cpubenchmark.net • Podporující min.
Paměť	• 8x 64GB RDIMM,
Pevné disky pro data	• Šasi serveru musí pojmout 4x HDD, přístupných ve vyměnitelných hot-swap rámečcích • Rozhraní disků SAS12, SATA6, rotačních i SSD • Osazeny 2x 480 GB SSD, DWPD=1 v RAID1
RAID řadič disků	• Podpora SAS12, SATA6 disků. • Podpora RAID 0,1,10 • Sběrnici připojení k systému PCI-e Gen 4.
SAS HBA	• 2x SAS 12Gb HBA pro připojení diskového pole
PCI-e sloty	• volný min. 1x PCI-e 8x Gen4 slot

LAN konektivita	• 4 porty LAN 25GbE SFP28
Napájení a chlazení	• Server musí být vybaven redundantním napájením a chlazením, vyměnitelné za provozu. • Zdroje 1+1 , každý alespoň 800W, hot-plug
Management a monitoring	• Servery musí disponovat kompletním out-of-band managementem s dedikovaným LAN portem 1GBase-T. Interní web-GUI managementu pouze v HTML5, možnost ovládání pomocí CLI. • Management serveru nepožaduje instalaci agenta jak pro monitoring, tak pro update SW/FW/BIOS v jednotlivých HW komponentech serveru. Podpora HW profilů. Podpora IPv6. • Podpora hromadné konfigurace více serverů pomocí XML souborů (z USB, nebo síťovým PXE bootem), hesla v takovém souboru musí být hashovaná proti zneužití (zero touch deployment). • Server musí umožňovat „lock-out“ BIOSu a firmware jednotlivých komponent tak aby bylo zabráněno přepisu závadnou aktualizací. Je požadována funkcionalita secure-erase (zabezpečené smazání veškerých dat na serveru a jeho komponentách po jeho vyřazení) • Součástí managementu serveru musí být vestavěná funkcionalita call-home (server musí být schopen automatizovaného předávání závad a otevírání servisních požadavku na helpdesk výrobce)
Operační systém	• Microsoft Windows Server 2022 Datacenter 16 CORE
Záruka	• Je požadována záruka na dobu 60 měsíců s reakční dobou na založený incident do konce následujícího pracovního dne (NBD).
Požadavky zadavatele na implementaci	• Instalace serverů v určeném místě zadavatele a zapojení do sítě LAN • Instalace posledních stabilních firmware. • Instalace a konfigurace serverové virtualizace. • Konfigurace služby call-home. • Migrace původních serverů.

Zálohovací server – 1 ks

Provedení: rackmount 19“, výška max. 2U, plnovýsuvné ližiny včetně ramena pro vedení kabeláže

1 ks CPU – architektura x86 s 16 plnohodnotnými jádry. Taktovací základní frekvence min. 2 GHz, FSB min. 4400 MHz, min. 30 MB L3 cache celkem, **nebo** v testu na cpubenchmark.net minimálně 36000 bodů. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 core z důvodu licencování OS a aplikací.
Server musí být osaditelný min. 24x disky HDD a 2x disky na instalaci OS. Veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) musí být již nyní osazeny tak, aby server bylo možné funkčně osadit plným počtem HDD pouhým dodatečným vložením disků
Diskový řadič s podporou RAID-1, RAID-5, RAID-6 zálohovaný, vytvoření alespoň 3xRAID skupin, velikost cache min. 8GB, rychlost 12Gbit/s
RAM 512 GB, RDIMM, 4800MT/s, Dual Rank
2 ks disků 480GB SSD HOTSWAP pro instalaci OS - konfigurace RAID-1 na samostatném HW řadiči
8 ks disků 3.84 SSD HOTSWAP
10 ks disků 16TB SAS 7.2K Enterpise, HOTSWAP - možnost rozšíření až na dvojnásobek pouhým vložením dalších disků.
2 ks Ethernet adapter Dual Port 10/25GbE SFP28 Adapter, RoCE v2, DCB. Karty budou od stejného výrobce se stejnou produktovou řadou.
2x SAS 12Gb HBA
2 ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení
Operační systém Microsoft Windows Server 2022 Datacenter 16 CORE
Server musí být osazen TPM 2.0
Redundantní hotswap ventilátory
IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient HTML5, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů)
Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB
Záruka 36 měsíců NBD onsite s možností rozšíření o dalších 24 měsíců. Přístup k firmware a jeho aktualizacím po dobu trvání záruční lhůty

Implementace:

1) Instalace serveru v určeném místě zadavatele a zapojení do stávající sítě LAN.
2) Instalace posledních stabilních firmware.
3) Instalace a konfigurace operačního systému.

1 ks - Hardened storage pro zálohy

Provedení: rackmount 19“, výška max. 2U, plnovýsuvné ližiny včetně ramena pro vedení kabeláže
1 ks CPU - architektura x86 s 16 plnohodnotnými jádry. Taktovací základní frekvence min. 2 GHz, FSB min. 4400 MHz, min. 30 MB L3 cache celkem, **nebo** v testu na cpubenchmark.net minimálně 36000 bodů. Max. počet CPU je omezen na 1 a počet jader je omezen na 16 core z důvodu licencování OS a aplikací
Server musí být osaditelný min. 24x disky HDD a 2x disky na instalaci OS. Veškeré potřebné komponenty (řadič, diskové pozice, kabeláž, napájecí zdroje apod.) musí být již nyní osazeny tak, aby server bylo možné funkčně osadit plným počtem HDD pouhým dodatečným vložením disků
Diskový řadič s podporou RAID-1, RAID-5, RAID-6 zálohovaný, vytvoření alespoň 3xRAID skupin, velikost cache min. 8GB, rychlost 12Gbit/s
RAM 64GB, RDIMM, 4800MT/s, Dual Rank
2 ks disků 480GB SSD HOTSWAP pro instalaci OS - konfigurace RAID-1 na samostatném HW řadiči
12 ks disků 16TB SAS 7.2K Enterpise, HOTSWAP - možnost rozšíření až na dvojnásobek pouhým vložením dalších disků.
2 ks Ethernet adapter Dual Port 10/25GbE SFP28 Adapter, RoCE v2, DCB. Karty budou od stejného výrobce se stejnou produktovou řadou.
2 ks hot-swap zdroje napájení dimenzované pro plné osazení serveru disky, CPU, RAM a PCIe zařízení
Server musí být osazen TPM 2.0
Redundantní hotswap ventilátory
IPMI 2.0 popř. obdoba, možnost vzdáleného převzetí grafické konsole bez závislosti na OS, webový klient HTML5, vzdálený mount DVD media, USB, dedikovaný port (není součástí požadovaného počtu ethernet portů)
Vyčítání přes SNMP celkového zdraví serveru bez nutnosti instalovat OS – jeden parametr v MIB
Záruka 36 měsíců NBD onsite s možností rozšíření o dalších 24 měsíců. Přístup k firmware a jeho aktualizacím po dobu trvání záruční lhůty

Implementace:

1) Instalace serveru v určeném místě zadavatele a zapojení do stávající sítě LAN.
2) Instalace posledních stabilních firmware.
3) Instalace a konfigurace operačního systému.

Zálohovací pásková knihovna – 1 ks

Požadavek na funkcionalitu – Zálohovací pásková knihovna
Formát knihovny
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 knihovny na pásková média
Minimálně 40 slotů, včetně případných potřebných licencí.
Příslušenství knihovny
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.
Požadavky na implementaci
Instalace páskové knihovny v určeném místě zadavatele a zapojení do stávající sítě LAN.
Instalace posledního stabilního firmware.
Připojení k dodávanému serveru.
Konfigurace včetně nastavení v zálohovací platformě.

Záruka a technická podpora
Standardní záruka v délce min. 36 měsíců poskytovaná přímo výrobcem zařízení.
Reakční doba do konce následujícího pracovního dne (NBD) od nahlášení na linku podpory.

Klientské licence operačních systémů

Požadované licence
Windows Server 2022 - User CAL (200 ks)
Windows Server 2022 - Device CAL (200 ks)
Windows Server 2022 - Remote Desktop User CAL (110 ks)

2 ks - Firewall NG

Základní technické požadavky

- Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, ...).
- Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let. Žádné z nabízených řešení nesmí být v době podání nabídky (uzavření smlouvy) v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky (uzavření smlouvy) součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
- Požadujeme dodání zařízení ve formátu HW appliance o velikosti 1 RU.
- Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACK.
- Možnost rozšíření platformy i další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž celé řešení musí být podporováno výrobcem.
- Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality.

HW parametry:

- Počet síťových rozhraní copper, RJ45 10/100/1000 - min 18x
- Počet 10 GE SFP+ - min 2x, včetně osazení všech portů SM zářičů 10 Gbit
- Počet GE SFP – min 4x
- Dedikovaný port RJ45 pro management
- Dedikovaný port RJ45 pro DMZ
- USB 3.0 port pro zálohu konfigurace
- Redundantní napájecí zdroj

Výkonnostní parametry:

- Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 18000 Mbps, 16000 Mbps, 9000 Mbps
- Výkon firewall – 14000000 paketů / s
- Počet naráz otevřených spojení – min 1.3 M
- Počet nových spojení za sekundu - min. 52 000

- Počet firewall pravidel až 10 000

Funkce:

Networking a High Availibility

- Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru
- Režim fungování L2 – transparentní režim, L3 – NAT/Router
- Podpora VLAN
- Podopora multicast, vytváření politiky pro multicast routování
- Podpora 802.3ad link aggregation
- Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading
- Podpora centrální NATovácí tabulky, stavová inspekce SCTP komunikace
- Podpora dynamických routovacích protokolů BGP, OSPF, ISIS
- Policy-based routing
- Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky

VPN

- **Funkce SSL VPN**
  - Podpora klientského i bezklientského (portálového) režimu
  - Minimální počet současně navázaných SSL VPN tunelů: 450
  - Minimální propustnost SSL VPN: 900Mbps
- **Funkce IPSEC VPN**
  - podpora site-to-site VPN
  - podpora klientských VPN
  - dostupnost VPN klienta pro koncové stanice (Windows, MacOS)
  - Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 100
  - Minimální počet klientských IPSEC VPN tunelů: 1000
  - propustnost IPSec VPN min. 11Gbps (měřeno při AES256-SHA256)
  - podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování
  - podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování
  - podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace
  - Podpora VXLAN
  - Podpora L2TP, PPTP, GRE
  - podpora dynamických routovací protokolů OSPF, BGP ve VPN IPsec

UTM

- **Funkce detekce aplikací na L7 (Application Control)**
  - Detekce známých aplikací na základě signatur
  - Signaturový database automaticky aktualizované výrobcem
  - pro populárná cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci)
  - možnost tvorby vlastních signatur
  - detekované aplikace je možné: povolit, monitorovat, blokovat
  - na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci
  - funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv.

NGFW pravidel popsaných výše.

- **Funkce detekce a potlačení narušení (IPS/IDS)**
  - signatury automaticky aktualizované výrobcem
  - možnost tvorby vlastních signatur
  - funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům
  - propustnost funkce IPS včetně logování min. 1500Mbps (měřeno na komunikaci typu mix aplikací)
- **Funkce antivirové kontroly**
  - Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem
  - Signatury automaticky aktualizované výrobcem
  - požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky)
  - možnost rozšíření o inspekci tzv. sandbox technikou formou lokálné HW appliance stejného výrobce
  - deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 650 Mbps
  - funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům.
  - Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů
  - Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu.
- **Funkce kategorizace webových stránek**
  - založená na centrálně spravované databázi výrobce
  - možnost definice vlastních kategorií
  - možnost definice vlastních seznamů zakázaných URL
  - kategorizace musí zahrnovat I české a slovenské internetové stránky
- **Funkce DNS filtru**
  - Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu)
  - Možnost definovat vlastní tzv. blacklist domén
  - Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL
  - Možnost importu seznamu blokovaných domén do DNS filtru
  - Detekce a blokování komunikace do botnet sítí
- **Funkce ochrany před únikem citlivých informací (DLP)**
  - možností analýzy běžných typů dokumentů a protokolů
  - možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum
  - Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty
  - Podpora SSL dekrypce/SSL inspekce s minimální propustností 900Mbps
  - DoS Policy prevence proti základním útokům typu DoS

Firewall

- Možnost nastavovat firewall politiku na základě geografických údajů
- Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem

- Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud
- Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru
- Viditelnost do provozu na aplikační úrovni
- Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo).
- Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu
- Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.
- Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii
- Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
- Podpora funkce reverzní proxy
- Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů
- **Explicit proxy**
    - podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)
    - podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos
    - funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta
    - Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru

Virtualizace

- Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.
- Každý virtuální kontext je zároveň samostatným wifi controllerem
- Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)

Management

- FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici
- Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě
- Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)

Bezplatný nárok na nové verze po dobu min. 3 roky

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

SW požadavky - Platforma pro centrální logování a reporting

- Virtuální appliance pro platformu VMware vSphere
- Virtuální appliance pro platformu Microsoft Hyper-V
- Plná podpora pro instalovanou platformu NGFW
- Podpora pro Syslog kompatibilní zařízení
- Výkon logování 6 GB / 1 den
- Kapacita storage pro logy 3 TB
- Podpora minimálně 4 virtuálních interface
- Real-time prohledávání logovaných dat
- 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 nabízenými firewally, 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 této zadávací dokumentace
- Event Management - upozorňování na důležité informace z logů – emailem 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
- Bezplatný nárok na nejnovější firmware po dobu min. 3 roky

Implementace

- Součástí dodávky je implementace do infrastruktury zákazníka.
- Konfigurace firewallu, migrace současných FW pravidel
- Konfigurace HA, VPN, IPSec

Poštovní server (1 ks)

Požadavek na funkcionalitu – Poštovní server
Požadované vlastnosti
Možnost provozu v on-premise nebo hybridním prostředí.
Podpora min. 256 GB paměti.
Podpora min. 24 procesorových jader.
Odesílání a přijímání elektronické pošty.
Sdílení kalendářů, kontaktů a úkolů.
Přístup přes https k informacím.

Adresářovou službou pro groupware systém je Active Directory.
Ochrana elektronické pošty proti virům a spamu.
Automatická konfigurace klientů.
Možnost off-line práce klienta.
Podpora protokolů MAPI, POP, IMAP, SMTP.
Možnost konfigurace groupware pro zajištění vysoké dostupnosti.
Škálovatelnost systémů od desítek po statisíce poštovních schránek.
Poštovní schránky typicky o velikosti 10 GB, kde velikost schránky je omezena jen dostupným diskovým prostorem.
Možnost použití levných SATA disků.
Integrovaný archivační systém pro poštovní systém.
Zabezpečená komunikace na bázi SSL a PKI.
Podpora TLS 1.2.
Šifrování e-mailových zpráv.
Ochrana dokumentů implementací transportních pravidel a DRM.
Ochrana informací a správa mobilních zařízení přistupujících k informacím.
Integrovaný monitoring poštovního provozu.
Centralizovaná správa.
Správa jak pomocí grafického rozhraní, tak i prostřednictvím příkazové řádky a skriptů.
Průvodci pro řešení problému, nástroje pro analýzu stavu systému.
Delegace oprávnění pro určité oblasti správy.
Prostředky pro řízení zdrojů (místnosti, projektory, automobily, ...).
Dynamické distribuční skupiny.
Globální i specificky zaměřené adresáře.
Klientská licence pro uživatele (200 ks).
Klientská licence pro zařízení (200 ks).
Požadavky na implementaci
Instalace poštovního serveru do nového virtuálního prostředí, na platformě Hyper-V
Instalace a konfigurace certifikátů.
Migrace dat z původního poštovního serveru, jedná se o migraci z Exchange serveru 2010, včetně přenastavení všech klientských emailových účtů.

Databázový server (1 ks)

Požadavek na funkcionalitu – Databázový server	Splňuje [Ano/Ne]
Technické požadavky	-
Podpora minimálně 24 jader.	
Minimálně 128 GB RAM na jednu instanci.	
Podpora základních Business Inteligence multidimenzionálních modelů.	
Režim úložiště v paměti.	
Minimálně 48 GB paměti na jednu instanci reportovacích služeb.	
Zabezpečení na úrovni řádků, maskování dat.	
Počet nodů failover clusteru – 2.	
Podpora asynchronní replikace do cloudového úložiště.	
Podpora komprese cloudové zálohy DB.	
Management nástroj na základě rolí v ceně produktu.	
Podpora hypervizoru pro virtualizaci.	
Nativní podpora XML.	
Licence na min. 4 procesorová jader, bez použití CALů, pro nasazení ve virtualizovaném prostředí.	
Požadavky na implementaci	-
Instalace databázového serveru do nového virtuálního prostředí.	
Migrace dat z původního serveru.	
Záruka a technická podpora	-
Standardní záruka v délce min. 36 měsíců.	

Součástí nabídky bude antivirový systém, který bude instalován v on-premise prostředí pro 400 poštovních schránek s podporou na 3 roky.

1, Antivirové, anti-spam, anti-phishing řešení pro poštovní server Exchange

- Implementace antivir, anti-spam, anti-phising bude na nově dodaném řešení a s tím integrováno
- Společná ochrana celého serveru – schránek i souborového systému serveru
- Podpora MS Exchange 2016 a novější
- Antivirus a antispyware

- Antispam s funkcí graylisting
- Blokace nevyžádané pošty a phishingu bez potřeby manuálně upravovat SCL (Spam Confidenace Level) hodnoty
- Kontrola jednotlivých MBX databází, případně konkrétní schránky uživatele
- Umožnit uživateli poštovní schránky pracovat pomocí samostatného prohlížeče se spamovými a potenciálně infikovanými zprávami, které nebyly doručeny do emailové schránky
- Možnost vlastních pravidel s vlastním hodnocením obsahu
- Detekce typu souborů v reálném čase
- Možnost správy přes příkazovou řádku
- Komplexní protokoly blokovaného spamu a zobrazení greylistingovaných odesílatelů ...protokoly všech zpráv, nejen blokovaných
- Sledování výkonu serveru v reálném čase
- Možnosti pro nastavení pravidel inspekce souborů – mazání spustitelných souborů, skriptů...
- Možnost využití cloudové reputační služby pro kontrolu příloh emailových zpráv
- Napojení na centrální správu
- Podpora více doménových prostředí
- Možnost exportu protokolu událostí produktu do protokolu operačního systému
- Tvorba pravidla "Z hlavičky" a vyhodnocovat pole From: pro přesnější detekci podvržených e-mailů
- Backscatter ochrana
- Synchronizace lokální karantény zpráv napříč uzly clusteru
- Podpora hybridního prostředí Office 365
- Možnost zasílání přehledů o zachycených e-mailových hrozbách koncovým uživatelům

2, Integrovaná cloudová analýza neznámých vzorků

- Funkce cloudového sandboxu je integrována do klienta pro poštovní server. Cloudový sandbox nemá vlastního agenta, nevyžaduje instalaci další komponenty ať už v rámci produktu nebo implementace HW prvku do sítě.
- Sandbox umožňující spuštění vzorků malwaru pro:
    - Windows,
    - Linux
- Analýza neznámých vzorků v řádu jednotek minut.
- Optimalizace pro znemožnění obejití anti-sandbox mechanismy.
- Schopnost analýzy rootkitů a ransomwaru.
- Schopnost detekce a zastavení zneužití nebo pokusu o zneužití zero day zranitelnosti.
- Řešení pracuje s behaviorální analýzou.
- Kompletní výsledek o zanalyzovaném souboru včetně informace o nalezeném i nenalezeném škodlivém chování daného souboru
- Manuální odeslání vzorku do sandboxu.
- Možnost proaktivní ochrany, kdy je potenciální hrozba blokována, dokud není znám výsledek analýzy ze sandboxu.
- Neomezené množství odesílaných souborů.
- Veškerá komunikace probíhá šifrovaným kanálem.
- Okamžité odstranění souboru po dokončení analýzy v cloudovém sandboxu
- Možnost volby, jaké kategorie souborů do cloudového sandboxu budou odcházet (spustitelné soubory, archivy, skripty, pravděpodobný spam, dokumenty atp.)
- Velikost odeslaných souborů do cloudového sandboxu může dosahovat až 64MB.

3, Centrální management konzole pro správu on-prem poštovních serverů

- Webová konzole
- Možnost probuzení klientů pomocí Push Notifications
- Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta
- Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu).
- Administrace v nejpoužívanějších jazycích včetně češtiny
- Široké možnosti konfigurace oprávnění administrátorů (například možnost správy pouze části infrastruktury, které konkrétnímu administrátorovi podléhá).
- Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA.
- Podpora štítků/tagování pro snazší správu a vyhledávání
- Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
- Vzdálené získání zachyceného škodlivého souboru z klienta.
- Detekce nespravovaných (rizikových) počítačů komunikujících na síti.
- Instalace a odinstalace aplikací 3. stran.
- Vyčítání informací o verzích softwaru 3. stran.
- Možnost vyčítat informace o hardwaru na spravovaných zařízeních (CPU, RAM, diskové jednotky, grafické karty...).
- Odeslání zprávy na počítač / mobilní zařízení, které se následně zobrazí uživateli na obrazovce.
- Vzdálená odinstalace antivirových řešení
- Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku.
- Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny a automatickému uplatnění klientské úlohy
- Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy).
- Podpora SNMP Trap, Syslogu
- Podpora instalace skriptem - *.bat, *.sh, *.ini (GPO, SSCM...).
- Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu.
- Reportování stavu klientů chráněných jinými bezpečnostními programy.
- Schopnost zaslat reporty a upozornění na e-mail.
- Přidání zařízení do vzdálené správy pomocí:
    - o synchronizace s Active Directory,
    - o ruční přidání pomocí dle IP adresy nebo názvu zařízení,
    - o pomocí síťového skenu nechráněných zařízení v síti.

2x core optický switch

- 48x SFP+ 1G/10G portů
- Min. 4x 40G/100G portů QSFP pro uplink
- Podpora redundantního napájení
- Zdroje vyměnitelné za provozu (hotplug)
- Monitorování a zabezpečení sítě v reálném čase~~,~~

- Podporuje protokol uplinku REUP a realizuje duální ochranu hardwaru
- Podpora protokolu IPv4/IPv6 dual-stack
- Podpora směrování VXLAN a přemostění VXLAN
- Monitorování zásad zabezpečení
- Správa - CLI, webová správa, cloud
- Podpora IPV6 VXLAN přes IPV4
- Podpora funkce M-LAG
- Podpora OpenFlow 1.3
- FTP
- NTP
- SNTP
- Podpora DLDP
- Podpora technologie rychlého přepínání REUP dual-link
- Základy směrování IPv4
- SNMP/v2/v3
- RMON
- SSHv2
- Správa nahrávání a stahování souborů FTP/TFTP
- Podpora protokolu NTP
- Podpora Syslog
- Podpora SPAN/RSPAN/ERSPAN
- Podpora telemetrie
- Podpora ZTP
- Podpora NETCONF
- Podpora Python
- Anti-DDoS útok
- DHCP Snooping
- Anti-Gateway ARP Spoofing
- Kontrola ARP
- Podpora správy klasifikace uživatelů
- Detekce nelegálních paketů a šifrování dat
- Anti-source IP spoofing
- Anti-IP skenování
- Podpora RADIUS/TACACS
- Filtrování paketů ACL VLAN IPv4/v6
- Minimální - switching kapacita 4.8T/96T
- Spanning Tree Protocols - IEEE802.1d STP, IEEE802.1w RSTP, Standard 802.1s MSTP, Port fast,
- VLAN - 4K 802.1q VLANs, Port-based VLAN, MAC-based VLAN, Protocol-based VLAN, Private VLAN, Voice VLAN, QinQ, IP subnet-based VLAN,GVRP
- 4x stackovací kabel 40G 5m

Optické transievery:

- 20x 10GBASE-ER, SFP+ Transceiver
- 10x 1000BASE-TX, SFP Transceiver
- 8x QSFP+ Transceiver
- 12x 1000BASE-ZX, SFP Transceiver

10x koncový switch pro endpointy s PoE

- 48x 10/100/1000BASE-T PoE+ min PoE budget 1480W
- 4x 1G/10G SFP+
- 1 MGMT port, 1 console port, and 1 USB port, compliant with USB2.0 standard
- 2x napájecí zdroj
- Switching kapacita min 1.36Tbps/13.6Tbps
- ACL - Standard/Extended/Expert ACL, Extended MAC ACL, ACL 80, IPv6 ACL, ACL logging, ACL counter, ACL remark, Global ACL, ACL redirect
- QoS - 802.1p/DSCP/TOS traffic classification; Multiple queue scheduling mechanisms
- VLAN - 4K 802.1q VLANs, Port-based VLAN, MAC-based VLAN, Protocol-based VLAN, Private VLAN, Voice VLAN, QinQ, IP subnet-based VLAN, GVRP
- Link Aggregation - AP, LACP, Flow balance
- Spanning Tree Protocols - IEEE802.1d STP, IEEE802.1w RSTP, Standard 802.1s MSTP,
- DHCP - DHCP server, DHCP client, DHCP snooping, DHCP relay, IPv6 DHCP snooping, IPv6 DHCP client, IPv6 DHCP relay
- Multiple Spanning Tree Protocol (MSTP)
- L2 Features -MAC, EEE, ARP, VLAN, Link aggregation, Mirroring, STP, RSTP, MSTP, Broadcast storm control,
- Layer 2 Protocols - IEEE802.3, IEEE802.3u, IEEE802.3z, IEEE802.3x, IEEE802.3ad, IEEE802.1p, IEEE802.1x, IEEE802.3ab, IEEE802.1Q (GVRP), IEEE802.1d, IEEE802.1w, IEEE802.1s
- Security - Binding of the IP address, MAC address, and port address; Binding of the IPv6, MAC address, and port address; Filter illegal MAC addresses; Port-based and MAC-based 802.1x;

10x koncový switch pro endpointy

- 48x 10/100/1000BASE-T
- 4x 1G/10G SFP+
- 1 MGMT port, 1 console port, and 1 USB port, compliant with USB2.0 standard
- 4x 10G SFP+ a 2x 40G/100G QSFP+
- 2x napáejcí zdroj
- Switching kapacita až 1.36Tbps/13.6Tbps
- ACL - Standard/Extended/Expert ACL, Extended MAC ACL, ACL 80, IPv6 ACL, ACL logging, ACL counter, ACL remark, Global ACL, ACL redirect
- QoS - 802.1p/DSCP/TOS traffic classification; Multiple queue scheduling mechanisms, such as SP, WRR, DRR, SP+WFQ, SP+WRR, SP+DRR; Input port-based speed limit; Port-based traffic recognition; Each port supports 8 queue priorities
- VLAN - 4K 802.1q VLANs, Port-based VLAN, MAC-based VLAN, Protocol-based VLAN, Private VLAN, Voice VLAN, QinQ, IP subnet-based VLAN, GVRP
- Link Aggregation - AP, LACP, Flow balance
- Spanning Tree Protocols - IEEE802.1d STP, IEEE802.1w RSTP, Standard 802.1s MSTP, Port fast, BPDU filter, BPDU guard, TC guard, TC filter, TC protection, LOOP guard, ROOT guard
- DHCP - DHCP server, DHCP client, DHCP snooping, DHCP relay, IPv6 DHCP snooping, IPv6 DHCP client, IPv6 DHCP relay
- L2 Features -MAC, EEE, ARP, VLAN, Link aggregation, Mirroring, STP, RSTP, MSTP, Broadcast storm control, DHCP, Jumbo frame, LLDP, Layer 2 protocol tunnel.
- Layer 2 Protocols - IEEE802.3, IEEE802.3u, IEEE802.3z, IEEE802.3x, IEEE802.3ad, IEEE802.1p, IEEE802.1x, IEEE802.3ab, IEEE802.1Q (GVRP), IEEE802.1d, IEEE802.1w, IEEE802.1s
- Security - Binding of the IP address, MAC address, and port address; Binding of the IPv6, MAC address, and port address; Filter illegal MAC addresses; Port-based and MAC-based 802.1x; MAB; Portal and Portal 2.0 authentication; ARP-check; DAI; Restriction on the rate of ARP packets; Gateway anti-ARP spoofing; Broadcast suppression; Hierarchical management

by administrators and password protection; RADIUS and TACACS+; AAA security authentication (IPv4/IPv6) in device login management; SSH and SSH V2.0; BPDU guard;

1x kontroler pro bezdrátové AP – centrální správa přístupových bodů

- Možnost přepínání mezi centralizovaným a lokálním přesměrováním
- dynamické přidělování šířky pásma pro STA, výběr pásma 5G, plynulé síťové připojení
- Podpora min. 64x AP
- 8x GE combo porty a 4x 10GE SFP+
- Zabezpečená WiFi pro hosty
- PPSK Enterprise Authentication
- Pre-AX, CorrectLink & AirReorder Funkce pro Wi-Fi s vysokou hustotou
- Technologie vzdáleného inteligentního vnímání (RIPT)
- Non-stop servis během upgradu
- Podpora licencování všech AP
- V případě licencování pokrytí licencí min. 64 AP
- Min. spravovatelných AP 64
- Min. počet klientů 30 000
- Min. počet WLAN ID: 4 000
- Min. počet záznamů MAC adres 130 000

50x Bezdrátové AP s připojením do centrálního kontroleru

- WiFi 6
- Protokoly: 802.11a/n/ac/ax a 802.11b/g/n/ax
- 4x4 MU-MIMO
- PoE
- 1x 10/100/1000 BASE-T
- 1x 2.5G SFP/SFP+
- Flexibilní možnosti správy
- Dual-radio dual-band:
- Rádio 1: 2,4 GHz 11ax, 2×2 MIMO
- Rádio 2: 5 GHz 11ax, 2×2 MIMO
- Provozní pásmo - Rádio 1: 802.11b/g/n/ax, 2.4GHz～2.483GHz, HE40
- Rádio 2: 802.11a/n/ac/ax, 5.150GHz～5.350GHz, HE80/HE160
- 802.11a/n/ac, 5,470 GHz, 5,725 GHz, 5,725 GHz, 5,850 GHz, HE80

Maximální propustnost:

- Rádio 1: 2,4 GHz, 0,574 Gbps
- Rádio 2: 5 GHz, 2,402 Gbps
- Zisk antény 2,4 GHz: 3 dBi, 5GHz: 3dBi,
- Vysílací výkon 20 dBm
- Nastavitelný výkon 1dBm
- Modulace OFDM
- Maximální propustnost na AP: 2,4 GHz + 5 GHz, 2,976 Gbps
- 1x 10/100/1000M Ethernet port BASE-T
- PoE (podpora IEEE 802.3af/at)
- Full Spectrum Provoz v režimu IEEE 802.3af

- 1x 1G/2,5G SFP port
- Port pro správu RJ45 (Konzole)
- LED indikátor
- Tlačítko reset
- Max Spotřeba energie 14W
- Doporučený počet klientů 120
- Skrytí SSID
- Priorita 5G (pásmové řízení)
- Podpora PSK a webové ověřování
- Podpora - Šifrování dat: WPA2 (AES), WPA3,
- Podpora - Ověření PPSK
- Podpora - Ověření 802.1X
- Podpora - Ověření PEAP

Zálohovací software

Nabízený SW musí umožnit zálohovat virtualizované prostředí Zadavatele, které je provozováno ve dvou lokalitách, serverovnách. Uchazeč nabídne řešení trvalou licencí, která umožní zálohovat minimálně 50 ks virtualizovaných serverů.
Zálohovací software musí pracovat s infrastrukturou Hyper-V 2016 a Hyper-V 2019, Hyper-V Windows server 2022
Nabízený SW pro zálohování musí mít v ceně SW updaty a základní podporu na dobu min. 5 let
Software musí podporovat hostitele Hyper-V
Software musí podporovat zálohování všech operačních systémů, které jsou podporovány pro provoz v Hyper-V
Software musí podporovat zálohování sdílených souborů ze zařízení založených na NAS pomocí sdílených složek SMB / CIFS a NFS a přímo ze souborových serverů Windows a Linux.
Software musí být nezávislý na hardware a musí využívat jakýkoli hardware serveru a úložiště
Software musí vytvářet samostatné zálohovací archivy ve formě souborů, které jsou volně přenositelné, s možností vytvářet takové soubory na úrovni zálohovací úlohy nebo na VM
Software musí umožňovat vytváření záloh v plném, syntetickém úplném, přírůstkovém a režimu
Software musí mít mechanismy deduplikace a komprese, které vedou ke snížení objemu úložného prostoru pro zálohy. Povolení deduplikace a / nebo komprese nesmí omezit žádné funkcionality obnovy dat, uvedené v této specifikaci
Software musí podporovat přímé zálohování do S3 kompatibilních objektových úložišť pro všechny typy podporovaných virtualizačních, cloudových i fyzických platforem, včetně NAS zařízení – uvedené zadavatel požaduje na základě předpokladů externího zálohování na objektová uložiště /cesnet/
Software musí poskytovat abstrakční vrstvu přes jednotlivá úložná zařízení, aby se vytvořil jeden virtuální fond záložního úložiště pro ukládání záloh. Musí být podporováno neomezené množství extentů. - uvedené zadavatel požaduje na základě předpokladů externího zálohování na objektová uložiště /cesnet/
Software musí umožňovat ochranu proti smazání a změně (immutability) pro objektové úložiště
Poškození, nebo ztráta zálohovacího serveru, či jeho databáze nesmí mít žádný vliv na obnovitelnost zálohovaných dat.
Software NESMÍ vyžadovat instalaci jakéhokoli druhu stálého agenta uvnitř virtuálních počítačů, který by byl nezbytný pro možnost vytvoření zálohy, nebo granulární obnovu souborů, či aplikačních položek
Software musí umožňovat „single pass backup“ s možností vyloučit zpracování jednotlivých souborů a složek. „Jednoprůchodová záloha“ musí být postačující pro všechny druhy obnovení včetně granulárních obnov na úrovni aplikací
Software musí umožnit instalovat, konfigurovat a řídit zálohování platforem Microsoft Azure, on-premise instalace zálohovacího řešení
Software musí umožňovat připojování a spouštění jakéhokoli skriptu pro zálohování před nebo po spuštěním zálohovací úlohy, nebo před a po snapshotu VM
Software musí nabízet samoobslužný portál, prostřednictvím kterého si uživatelé mohou obnovit soubory, virtuální počítače, objekty MS Exchange a databáze MS SQL, (včetně obnovení ke konkrétnímu bodu v čase)
Software musí být schopen integrace s jinými systémy pomocí zabudovaného rozhraní REST API
Software musí nabízet šifrování celého síťového provozu mezi všemi komponentami a také šifrování "na cíli" záložních souborů v úložišti.
Software musí mít architekturu klient / server s možností instalace více instancí administrativní konzoly
Přístup na administrativní konzoly musí být chráněn multi-faktorovou autentizací (MFA)
Software musí využívat mechanismus sledování změněných datových bloků. Pro všechny podporované hypervizory musí být implementace CBT certifikována výrobcem hypervizoru

Software musí nabízet způsoby, jak omezit stres na produkčním úložišti během zálohování tak, aby záloha kontrolovatelným způsobem ovlivňovala latenci produkčního úložiště.
Výše uvedená funkce musí být konfigurovatelná na úrovni datastore virtualizační platformy
Software musí nabízet automatickou detekci "orphaned snapshots" a musí provést jejich konsolidaci automaticky bez zásahu uživatele
Software musí umožňovat vytváření záloh integrací se snímky (snapshot) externí úložiště dat
Řešení musí umožňovat orchestraci snímků diskových polí a jejich vytváření se zajištěním aplikační konzistence
Řešení musí umožnit obnovu jednotlivých VM, souborů a položek aplikací přímo ze snímků diskových úložišť.
Software musí podporovat NDMP protokol pro zálohování NAS zařízení
Podobná funkcionalita musí být zajištěna pro úložiště založená na souborovém systému Linux XFS
Software musí být schopen kopírovat body obnovení a replikovat virtuální počítače do vzdáleného umístění pomocí technologie založené na vestavěné akceleraci WAN
Software musí umožňovat uchování více bodů obnovení na replikačních virtuálních počítačích
Software musí umožňovat „seeding“ replik ze stávajícího virtuálního počítače
Software musí mít stejné funkce replikace pro Hyper-V
Software musí využívat všechny režimy přenosu zálohy podporované hypervizorem (network, hotadd, direct SAN a direct NFS)
Software musí být schopen vytvořit zálohu „ad-hoc“ pomocí nativní konzole nebo webového klienta vSphere
Software musí umožňovat paralelní zpracování virtuálních disků a jejich disků, včetně paralelní obnovy virtuálních disků v úplném režimu obnovy VM
Software musí umožňovat okamžitou obnovu více virtuálních strojů současně, přímo ze záložních souborů z libovolného bodu obnovení (vestavěný NFS server). Tato funkce musí být podporována pro prostředí Hyper-V a musí fungovat bez ohledu na hardware používaný k ukládání záložních souborů VM
Software musí umožňovat online migraci virtuálních počítačů, které běží tímto způsobem, do produkčního úložiště pomocí funkcí hypervizoru. Řešení musí také poskytovat svou vlastní funkci, která takové schopnosti poskytne.
Software musí umožňovat úplné obnovení VM, obnovu souborů VM nebo disků VM
Software musí umožňovat úplné obnovení VM přímo do Microsoft Azure, prostředí MS azure se již využívá pro část emailových služeb.
Software musí umožňovat obnovu souborů na stroj operátora nebo přímo do produkční VM bez potřeby agenta nainstalovaného uvnitř VM. Během obnovy bez agentů nesmí existovat žádné omezení na velikost souboru ani omezení počtu souborů
Software musí umožňovat obnovu souborů přímo do virtuálního počítače pomocí síťového připojení a rozhraní VIX API v PowerShell Direct v prostředích Hyper-V
Software musí umožňovat okamžitou obnovu prostředí ze zálohy NAS pomocí protokolu CIFS/SMB.
Software musí podporovat obnovu souborů z Linux LVM a Windows Storage Spaces
Software musí umožňovat rychlou a podrobnou obnovu aplikačních objektů bez použití jakéhokoli agenta nainstalovaného uvnitř virtuálních počítačů
Software musí podporovat granulární obnovení libovolného objektu a všech atributů tohoto objektu včetně hesla, GPO, AD configuration partition, AD integrovaných záznamů DNS, Microsoft System Objects, informací o certifikátu CA a AD Sites subnet
Software musí podporovat Microsoft Exchange 2013 a novější, granulární obnovení jakéhokoli objektu včetně objektů ve složce „Permanently deleted objects“
Software musí podporovat granulární obnovení Microsoft SQL 2008 SP4 a novějších, včetně databází s možností obnovení v čase (PiT), obnovy na úrovni tabulky, schéma – využváno MSSQL
Software musí podporovat podrobné obnovení Microsoft Sharepoint Server 2013 a novějších. Možnost obnovit položky, weby, oprávnění – využíván sharepoint
Software musí umožňovat publikování MS SQL přímo ze záložního souboru na spuštěný databázový server
Software musí umožňovat okamžitou obnovu databází MS SQL v režimu Instant Recovery do libovolného umístění.
Software musí umožňovat „reverzní CBT“ a obnovu pomocí Direct SAN
Software musí umožňovat vytváření virtuální laboratoře (izolovaného prostředí) pro infrastrukturu Hyper-V pomocí VM spuštěných přímo ze záložních souborů.
Software musí mít mechanismy ověřování obnovení zálohy umožňující testování obnovy virtuálních počítačů v izolovaném síťovém prostředí na infrastruktuře Hyper-V. Ověření musí umožňovat testování aplikace uvnitř VM pomocí vlastních nebo předdefinovaných skriptů. Ověření musí být naplánovatelné a zcela automatizované

Software musí být před obnovením produkčních prostředí integrován s antivirovým softwarem, aby bylo možné skenovat zálohu na úrovni image disků. Skenování musí být provedeno na souborovém systému v záložním souboru, aniž by bylo nutné předem extrahovat data. Integrace musí zahrnovat alespoň Windows Defender,
Software musí umožňovat automatizovanou dvoustupňovou obnovu virtuálních strojů, což umožňuje vložení vlastních skriptů za účelem změny dat před obnovením do produkčního prostředí.