VZLU AEROSPACE, a.s.
Beranových 130, 199 00 Praha - Letňany
OR : Městský soud v Praze,oddíl B,vložka 446
IČO: 00010669 DIČ: CZ00010669
Bankovní spojení : [redacted]

OBJEDNÁVKA

Číslo : OV4250047/2

Zakázka : SVR027
Středisko : 2000
Počet listů : 1

STORAGE ONE, a.s.

Jeremiášova 957/16
15500 Praha 5

Vyřizuje / linka: [redacted]

Praha - Letňany
12.02.2025

P.č.	Množství / M.j.	Specifikace	Cena bez DPH
1	1,00 ks	Objednáváme u vás: DLP: Data Loss Prevention Licence na 3 roky, funkcionalita popsána viz. přílohy Termín dodání : 14.03.2025 Platební podmínky : bankovním převodem Dodací podmínky : dodat na adresu firmy /7.00 - 13.00 h/ **Fakturace na roční bázi!** Na daňovém dokladu (dodacím listu) uvádějte prosím č. naší objednávky. Žádáme Vás o potvrzení přijaté objednávky včetně termínu dodání a ceny. V případě vystavení zálohové faktury Vás žádáme o zaslání daňového dokladu o přijaté platbě (dle zákona o DPH č.235/2004 Sb., §26). FAKTURY PROSÍM ZASÍLEJTE EMAILEM NA: [redacted] VZLÚ je povinným subjektem dle zákona č. 340/2015 Sb. o registru smluv. Smlouva/objednávka, mimo části podléhající obchodnímu tajemství, bude v souladu s tímto zákonem uveřejněna v registru smluv. Smlouva/objednávka nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv. Objednatel se zavazuje tuto smlouvu/objednávku bez zbytečného odkladu po jejím podpisu oběma smluvními stranami, zaslat správci registru smluv k uveřejnění	[redacted]

Razítko a podpis : [redacted]

Razítko [redacted]

Telefon : [redacted]

e-mail: [redacted]

Popis požadovaných vlastností systému DLP (Data Loss Preventition)

DLP (Data Loss Prevention) je systém, který organizacím pomáhá chránit citlivá data před neautorizovaným sdílením či únikem. Základem DLP je identifikace důležitých informací (například osobních údajů, finančních dat nebo duševního vlastnictví) a neustálé sledování jejich pohybu v rámci firemních sítí, cloudových prostředí a koncových zařízení.

Technické vlastnosti

Správa

- Jednotná centrální konzole pro správu (požadovaná možnost instalace on-premise)
    - Přístup přes webové rozhraní https s možností využití certifikátu podepsaného interním CA
    - Přehled systémů v síti
    - Synchronizace s AD, LDAP
    - Možnost vytvoření statistik (připravených i vlastních) nad monitorovanými akcemi a zařízeními
    - Podpora rychlého přehledu (Dashboard)
    - Instalace, nastavení a reporting pro veškeré produkty
    - Definice intervalu aktualizace politik a zasílání událostí
    - Pravidla definovaná pro uživatelské skupiny, konkrétní uživatele a organizační jednotky (nebo kombinace vícero parametrů) definované v adresářové struktuře AD/LDAP
    - Přístup k logům, dashboardům a správě politik řízení na základě rolí a uživatelské indentity v AD a podporou autentizace pomocí klientských certifikátů
    - Možnost integrace s více AD doménami, volitelná frekvence synchronizace informací
    - Definice privilegovaných uživatelů bez blokací definovaných politikou (jen monitoring)
    - Politiky definované pro online a offline klienty (připojení do sítě i odpojení od ní)
    - Politiky zpětně kompatibilní se staršími verzemi
    - Podpora REST API
    - Propojení na SIEM

Agent

- Integrace DLP a Device Control do jednoho DLP host agenta
- Management agent může být instalován z centrální konzole, manuálně, skrze nástroj třetích stran a může být integrován v připravených instalačních obrazech
- Agent umožňuje i správu ze stroje (pokud je povoleno centrální správou), přehled historie událostí pro uživatele, možnost vyžádání dočasného vypnutí určité bezpečnostní politiky (centrální správa musí schválit)

Kontrola připojených zařízení

- Nastavení základních pravidel pro práci s připojenými zařízeními (fyzicky, ale i přes Bluetooth) je koncovému stroji
- Centrální správa přes ePo
- Bere v potaz GROUPS (vlastní skupina uživatelů, synchronizace s AD) a DEFINITIONS (připravené, ale i vlastní – například: čtečka SD karet, USB disky)
- Vlastní zařízení užité v pravidle jako nová položka DEFINITIONS nadefinovat na základě:
    - USB/PCI Vendor a Device ID
    - Výrobce
    - Modelu
    - Názvu
    - Výrobního čísla
    - Typu filesystému (NTFS, FAT, CDFS, UDFS)
    - Přístupu k filesystému (ro, rw)
    - Definované sběrnice (USB, PCI, SCSI, PCMCIA, IDE/SATA, Firewire, Bluetooth)
- Lze udělit výjimky:
    - Pro daná sériová čísla
    - Uživatele,
    - Procesy
    - Device templates.
- Reakční pravidla pro dané připojené zařízení (vždy nastaveno jak pro PC v síti, tak i pro PC odpojeného od sítě):
    - No action
    - Block
    - Read Only
- Možnost nastavení notifikace uživatele (vlastní logo, vlastní nebo předpřipravený text). Toto notifikace uživatele bude použita jak forma edukace pro zvýšení povědomí o bezpečnostních směrnicích.
- Možné typy pravidel:
    - TrueCrypt Device Rule
    - Removable Storage File Access Rule

    - Removable Storage Device Rule
    - Plug and Play Device Rule
    - Fixed Hard Drive Rule
    - Citrix XenApp Device Rule

Klasifikace dat

- Možnost využití výchozích předdefinovaných klasifikací
- Možnost vytvoření vlastní klasifikace
- Klasifikace na základě:
    - Obsahu dat:
        - Použití klíčových slov
        - Slovníků – možnost nahrát vlastní nebo použít výchozí
        - Advanced pattern – identifikuje data na základě jejich charakteristik, možnost nahrát vlastní nebo použít výchozí, definice pomocí regulárních výrazů
        - Exact data matching – dokument obsahuje konkrétní data
        - Proximity – porovnání slovníků, jejich shody apod.
    - Vlastnosti souborů:
        - Šifrování
        - Typy souborů (true type type)
        - Koncovky souborů
        - Umístění
        - Aplikace (executable file name/has, pracovní adresář, název)
        - Vycházející z DEFINITION (možnost použití výchozí nebo vlastní – např. source code, soubor určité velikosti, typu nebo určitého data vytvoření).
- V DPLP a DC politikách nastavení akcí pro dané KLASIFIKACE
- Manuální i automatická klasifikace
- Nastavení timeout strategie pro kontrolu pravidel a klasifikací

Ochrana koncové stanice pomocí agenta

- Monitoruje, identifikuje a případně blokuje aktivity s daty na koncových stanicích
- Skenuje lokální úložiště stroje a klasifikuje uložené dokumenty
- Pokrytí všech hlavních vektorů interních úniků dat.
- Centrální správa přes ePO
- Dostupnost pro Windows i Mac
- KLASIFIKACE DAT – vytvoření vlastních, použití výchozích (viz bod výše)
- Na základě KLASIFIKACÍ DAT se vytváří pravidla, možnost nastavení dle GROUPS, DEFINITIONS, možnost udělení výjimky
- Obsahová pravidla – na základě KLASIFIKACÍ – viz výše

    - Pro textové řetězce s podporou regulárních výrazů
    - S podporou slovníků včetně normativů (HIPAA, SOX, PCI GLBA)
    - Procházení celého dokumentu, těla, hlavičky a patičky
- Podpora pro Digital Rights Management (DRM)
    - Microsoft RMS
    - Seclore IRM
- Integrace s třetí stranou:
    - Adobe Acrobat Pro
    - Adobe Reader
    - Firefox
    - Lotus Notes client software
    - Microsoft .NET
    - Microsoft Internet Explorer
    - Prohlížeče – Microsoft Edge, Google Chrome, MSIE, Firefox
    - Microsoft Office
    - Microsoft Outlook
    - Microsoft Sharepoint
    - TrueCrypt
    - Seclore
    - Titus
    - Boldon James API
- Možné typy pravidel:
    - Ochrana snímání obrazovky – screen capture
    - Clipboard ochrana – v paměti
    - Ochrana dat nahrávaných na cloud:
        - Box
        - Dropbox
        - Google Drive
        - iCloud
        - OneDrive
        - Syncplicity
    - Ochrana dat posílaných e-mailem
    - Ochrana tisknutých dat
    - Ochrana dat nahrávaných na web včetně definice URL cesty obsahující query řetězec
    - Síťové komunikace (adresy, porty, směry komunikace)
- Pravidla s podporou minimálně 300 content types, zejména následujících:
    - Office dokumenty
    - Dokumenty ve formě PDF
    - Textové formáty a značkovací jazyky (TXT, CSV, HTML, XML)
    - Běžné archívy (ZIP, RAR, 7Z, ISO)

    - Šifrované dokumenty (PGP, S/MIME, ZIP, RAR, 7Z, Microsoft Office, OpenOffice.org, PDF)
    - Multimediální soubory
    - Zdrojové soubory
- Vyhledávání citlivých dat v :
    - Lokálním souborovém systému
    - E-mailovém úložišti (OST, PST)
- Podpora reakcí:
    - Monitoring
    - Evidence
    - Upozornění
    - Blokování
    - Vyžádání důvodu,
    - Smazání,
    - Zašifrování (součinnost s FRP a DriveEncryption)
- Z výše uvedených reakcí je možné nakonfigurovat různé možnosti chování. Například:
    - Tzv. tichý chod, kdy uživatel není notifikován ani blokován
    - Notifikace nebo blokace je uvedena lokalizovaným textem a definovanou grafikou
    - Požadavek na vysvětlení akce – uživatel může podat vysvětlí akce, kterou hodlá provést
- Policy Analyzer – při uložení pravidla dochází ke kontrole potenciálních problémů a dává rady jak správně nastavit a vyladit politiku
- Google Chrome Guest Mode Protection – umožní centrálně zakázat „guest mode“ v tomto prohlížeči
- Integrace klientského DLP a síťového DLP
- Podpora Citrix XenApp, WMwar View a Microsoft Terminal Services
- Ochrana lokální instalace

Síťové DLP

- Jednotná politika a nastavení klasifikace citlivých dat včetně definic vzorů pro všechny DLP systémy, pro host i network systémy
- Podpora běžných typů kódování
- DLP kontrola webového provozu i pro nespravované koncové systémy na úrovni sítě ve spolupráci s webovou bránou pomocí standardního protokolu ICAP.
- DLP kontrola e-mailového provozu i pro nespravované koncové systémy na úrovni sítě ve spolupráci s e-mailovou bránou pomocí standardního protokolu SMT a X-RCIS-Action header.
- Plná DLP kontrola webového a e-mailového provozu do propustnosti 150Mbps.

- Varianty appliace pro kontrolu webového a e-mailového provozu jako HW i virtuální applieance.
- Vyhledávání citlivých dat:
    - Na síťových úložištích CIFS, NFS, SharePoint
    - EMC Documentum
    - V databázích MS SQL, MySQL, Oracle
    - V cloudových uložištích SharePoint Online a Box
    - http(s), ftp(s)
    - Podpora OCR
- Reakce u nalezených citlivých dat na síťových úložištích mimo zaznamenání incidentu včetně důkazu:
    - Klasifikace souboru obsahující cilitvá data na úrovni file formátu
    - Vytvoření otisku pro jednotlivé fragmenty textu obsahu souboru s citlivými daty
    - Karanténa citlivých dat
    - Kopie citlivých dat na jiné definované úložiště
    - Přesunutí citlivých dat na jiné definované úložiště
    - Zašifrování citlivých dat dle politiky napčíklad klasifikace dat konkrétním šifrovacím klíčem
    - Aplikace Rights Management politiky
- Monitoring síťových komunikací na úrovni sítě přes TAP či SPAN s podporou:
    - http
    - smtp
    - pop3
    - imap
    - ftp
    - telnet
    - irc
    - ldap
    - smb, smb2
    - SOCK i TLS/SSL u relevantních protokolů.
    - Monitoring a klasifikace až do propustnosti 200Mbps.
- Rozdělení funkcionalit sítového DLP do modulů:
    - DLP Discover – skenování dat v lokálních a cloudových úložištích, jejich klasifikace, vytvoření statistik
        - Inventory scan – sběr metadata, skenování souborových úložišť a databází, poskytuje široký přehled o uložených datech
        - Classification scan – prochází databáze a souborová úložiště a klasifikuje data

        - Remediation scan – skenuje databáze a souborová úložiště, hledá data, která nejsou v souladu s politikami – možnost přemístit klasifikovaná data z neadekvátního úložiště do karantény.
    - DLP Prevent – v kombinaci s proxy systémy kontroluje a popřípadě blokuje e-mailovou a webovou komunikací (nutná podpora header inspection)
    - DPL Monitor – monitorování pohybu dat v síti a jejich analýza (objem, typ apod.)
- DLP Capture – funkcionalita používaná s DLP Monitor a DLP Prevent – uložená analyzovaných dat do cache umožňující následní testování politik.

storage one

Předběžná nabídka – průzkum trhu - DLP

Zpracováno pro: VZLU AEROSPACE, a.s.

1 Popis dokumentu

Název dokumentu:	**Předběžná nabídka – průzkum trhu - DLP**
Zpracováno pro:	**VZLU AEROSPACE, a.s.**
Datum předložení:	**10.02.2025**
Předkladatel:	**STORAGE ONE, a.s.**
Počet příloh:	**0**
Vedoucí projektu:	[redacted]

storageone.cz

5 Závěr

Společnost STORAGE ONE, a.s. prohlašuje, že všechny údaje uvedené v této předběžné nabídce jsou správné a úplné.

Společnost STORAGE ONE, a.s. je připravena Vám kdykoliv poskytnout dodatečné informace k obsahu této předběžné nabídky.

V Praze dne 10.2.2025

René Valvoda
předseda představenstva
STORAGE ONE, a.s.