ANUNȚ DE PARTICIPARE

privind achiziționarea de Licențe pentru produse program, abonamente la servicii software
(se indică obiectul achiziției)
prin procedura de achiziție Licitație deschisă
(tipul procedurii de achiziție)

1. **Denumirea autorității contractante:** ***Biroul Național de Statistică***
2. **IDNO:** ***1006601000200***
3. **Adresa:** ***mun. Chișinău, str. Grenoble 106***
4. **Numărul de telefon/fax:** ***022 403 125 / 022 403 127***
5. **Adresa de e-mail și de internet a autorității contractante:** ***moldstat@statistica.gov.md***
6. **Adresa de e-mail sau de Internet de la care se va putea obține accesul la documentația de atribuire:** ***Documentația de atribuire este anexată în cadrul procedurii în SIA RSAP***
7. **Tipul autorității contractante și obiectul principal de activitate (dacă este cazul, mențiunea că autoritatea contractantă este o autoritate centrală de achiziție sau că achiziția implică o altă formă de achiziție comună):** ***Nu se aplică***
8. **Cumpărătorul invită operatorii economici interesați, care îi pot satisface necesitățile, să participe la procedura de achiziție privind livrarea următoarelor bunuri:**

Nr. d/o	Cod CPV	Denumirea bunurilor solicitate	Cantitatea	Specificarea tehnică deplină solicitată, Standarde de referință	Valoarea estimată (fără TVA)
		LOTUL I. Licență antivirus			
1	48000000-8	**Licență antivirus**	Minimum 12 luni	Conform Anexei nr.1	156 580,00
	Valoarea estimativă totală, fără TVA (Lot I)				**156 580,00**
		LOTUL II. Sistem monitorizare a echipamentelor TI			
2	48612000-1	**Sistem de monitorizare a echipamentelor TI din toată organizația, la nivel central și oficii teritoriale**	1 unitate (minimum 12 luni)	Conform Anexei nr.2	625 000,00
	Valoarea estimativă totală, fără TVA (Lot II)				**625 000,00**
	Valoarea estimativă totală, fără TVA a achiziției				**781 580,00**

9. **În cazul în care contractul este împărțit pe loturi un operator economic poate depune oferta (se va selecta):**
   1) Pentru mai multe loturi
10. **Admiterea sau interzicerea ofertelor alternative:** ***Nu se admite***
(indicați se admite sau nu se admite)
11. **Termenii și condițiile de livrare solicitați:** ***Timp de 30 (treizeci) zile calendaristice din data semnării și înregistrării contractului, cu livrarea la adresa Beneficiarului: mun. Chișinău, str. Grenoble 106.***
12. ***Termenul de valabilitate*** **a contractului:** ***31.12.2021***
13. **Contract de achiziție rezervat atelierelor protejate sau că acesta poate fi executat numai în cadrul unor programe de angajare protejată (după caz):** ***Nu se aplică***

(indicați da sau nu)

14. Prestarea serviciului este rezervată unei anumite profesii în temeiul unor acte cu putere de lege sau al unor acte administrative (după caz): ***Nu se aplică***

(se menționează respectivele acte cu putere de lege și acte administrative)

15. Scurta descriere a criteriilor privind eligibilitatea operatorilor economici care pot determina eliminarea acestora și a criteriilor de selecție; nivelul minim (nivelurile minime) al (ale) cerințelor eventual impuse; se menționează informațiile solicitate (DUAE, documentație):

Nr. d/o	Descrierea criteriului/cerinței	Mod de demonstrare a îndeplinirii criteriului/cerinței:	Nivelul minim/ Obligativitatea
1	DUAE	Semnat electronic de către operatorul economic	Obligatoriu
2	Oferta	Formularul F 3.1, semnat electronic de către operatorul economic	Obligatoriu
3	Extras de la Camera Înregistrării de Stat	Copie, semnată electronic de către operatorul economic	Obligatoriu
4	Certificat de atribuire a contului bancar	Copie, eliberată de banca deținătoare de cont, semnată electronic de către operatorul economic	Obligatoriu
5	Certificat de efectuare sistematică a plății impozitelor, contribuțiilor	Copie, semnată electronic de către operatorul economic	Obligatoriu
6	Raport financiar	Copie, semnată electronic de către operatorul economic	Obligatoriu
7	Formularul informativ despre ofertant	Formularul F 3.3, semnat electronic de către operatorul economic	Obligatoriu
8	Specificaţii tehnice	Original, semnat electronic de către operatorul economic, în conformitate cu formularul F 4.1	Obligatoriu
9	Specificații de preț	Original, semnat electronic de către operatorul economic, în conformitate cu formularul F 4.2	Obligatoriu
10	Confirmarea calității produsului	Certificatul de conformitate de la producător, semnat electronic de către operatorul economic	Obligatoriu
11	Garanția bancară	Original, semnat electronic de către operatorul economic, prevăzută în Formularul F 3.2	Obligatoriu
12	Garanția de bună execuție	La încheierea contractului, original, semnat electronic de către operatorul economic	Obligatoriu
13	Declarația privind conduita etică și neimplicarea în practici frauduloase și de	Original, semnat electronic de către operatorul economic	Obligatoriu

	corupere Formularul №145 din 24.11.2020		
14	Minim ani de experienţă specifică în livrarea bunurilor	3 ani	Obligatoriu
15	Neimplicarea în situaţiile descrise în art. 18 al Legii privind achiziţiile publice nr.131/2015	Declaraţie pe proprie răspundere, completată în conformitate cu Formularul F 3.5, semnat electronic de către operatorul economic	Obligatoriu

16. Motivul recurgerii la procedura accelerată (în cazul licitaţiei deschise, restrînse şi al procedurii negociate), după caz: ***Nu se aplică***

17. Tehnici şi instrumente specifice de atribuire (dacă este cazul specificaţi dacă se va utiliza acordul-cadru, sistemul dinamic de achiziţie sau licitaţia electronică): ***Nu se aplică***

18. Condiţii speciale de care depinde îndeplinirea contractului (indicaţi după caz): ***Nu se aplică***

19. Criteriul de evaluare aplicat pentru adjudecarea contractului: ***Cel mai bun raport calitate-preţ***

20. Factorii de evaluare a ofertei celei mai avantajoase din punct de vedere economic, precum şi ponderile lor:

Nr. d/o	Denumirea factorului de evaluare	Ponderea
1.	Preţ	60 puncte (60%) Pentru cel mai mic preţ se acordă punctajul maxim alocat. Pentru alte preţuri punctajul se va acordă conform formulei: P (puncte ofertă) = (Preţ minim / Preţul ofertei) x Punctajul maxim alocat
2.	Criterii de calitate: 1) Caracteristici constructive (caracteristicile principalelor componente, versiunea actualizată, etc.) - punctaj max. 15; 2) Caracteristici funcţionale (viteza de execuţie, randamentul, productivitatea, fiabilitatea, etc.) - punctaj max. 15; 3) Caracteristici economice (resurse, cheltuieli de exploatare, de întreţinere, etc.) - punctaj max. 10.	40 puncte (40%) Comisia decide locul participantului pe fiecare subcriteriu de calitate, de la 1 la 3, cu alocarea punctelor din 5 în 5: - Locul 1 - 15 puncte (10 p. pentru criteriul 3); - Locul 2 - 10 puncte (5 p. pentru criteriul 3); - Locul 3 - 5 puncte; Pentru participanţii rămaşi nu se acordă puncte. Punctele se însumează pentru fiecare participant, pe fiecare subcriteriu şi se reflectă în scorul final.
	TOTAL PUNCTAJ - 100 puncte (100%)	

21. Termenul limită de depunere/deschidere a ofertelor:

- **până la:** ***[0:00] Informaţia o găsiţi pe SIA RSAP***

- **pe:** ***Informația o găsiți pe SIA RSAP***

22. Adresa la care trebuie transmise ofertele sau cererile de participare:

Ofertele sau cererile de participare vor fi depuse electronic prin intermediul SIA RSAP

23. Termenul de valabilitate a ofertelor: ***60 zile***

24. Locul deschiderii ofertelor: ***SIA RSAP***

(SIA RSAP sau adresa deschiderii)

Ofertele întîrziate vor fi respinse

25. Persoanele autorizate să asiste la deschiderea ofertelor:
Ofertanții sau reprezentanții acestora au dreptul să participe la deschiderea ofertelor, cu excepția cazului cînd ofertele au fost depuse prin SIA "RSAP".

26. Limba sau limbile în care trebuie redactate ofertele sau cererile de participare:

Limba română

27. Respectivul contract se referă la un proiect și/sau program finanțat din fonduri ale Uniunii Europene: ***Bugetul de stat***

(se specifică denumirea proiectului și/sau programului)

28. Denumirea și adresa organismului competent de soluționare a contestațiilor:
Agenția Națională pentru Soluționarea Contestațiilor
Adresa: mun. Chișinău, bd. Ștefan cel Mare și Sfânt nr.124 (et.4), MD 2001;
Tel/Fax/e-mail: 022 820 652, 022 820 651, contestatii@ansc.md

29. Data (datele) și referința (referințele) publicărilor anterioare în Jurnalul Oficial al Uniunii Europene privind contractul (contractele) la care se referă anunțul respective (dacă este cazul): ***Nu se aplică***

30. În cazul achizițiilor periodice, calendarul estimat pentru publicarea anunțurilor viitoare: ***Nu se aplică***

31. Data publicării anunțului de intenție sau, după caz, precizarea că nu a fost publicat un astfel de anunţ: ***Nu a fost publicat un anunț de intenție***

32. Data transmiterii spre publicare a anunțului de participare: ***Conform SIA RSAP***

33. În cadrul procedurii de achiziție publică se va utiliza/accepta:

Denumirea instrumentului electronic	**Se va utiliza/accepta sau nu**
Depunerea electronică a ofertelor sau a cererilor de participare	Se acceptă
Sistemul de comenzi electronice	Se acceptă
Facturarea electronică	Se acceptă
Plățile electronice	Se acceptă

34. Contractul intră sub incidența Acordului privind achizițiile guvernamentale al Organizației Mondiale a Comerțului (numai în cazul anunțurilor transmise spre publicare în Jurnalul Oficial al Uniunii Europene): ***Nu se aplică***

(se specifică da sau nu)

Digitally signed by Cara Oleg
Date: 2021.06.15 16:41:06 EEST
Reason: MoldSign Signature
Location: Moldova

Conducătorul grupului de lucru: Oleg CARA _____

L.Ș.

Digitally signed by Valcov Vitalie
Date: 2021.06.15 13:55:28 EEST
Reason: MoldSign Signature
Location: Moldova

Digitally signed by Mîrzac Ion
Date: 2021.06.15 14:04:14 EEST
Reason: MoldSign Signature
Location: Moldova

Digitally signed by Hainițchi Tatiana
Date: 2021.06.15 15:06:10 EEST
Reason: MoldSign Signature
Location: Moldova

Soluție de protecție și securitate antivirus pentru protecția infrastructurii

Cerinte Generale

Disponibilitatea tehnologiilor de protecție împotriva software-ului rău intenționat care se răspândește prin rețele web, sisteme de poștă, medii de stocare și altele asemenea.

Disponibilitatea unui instrument de management centralizat (server de management) al parametrilor și setărilor de protecție împotriva amenințărilor pe stațiile de lucru client.

Prezența unei console de management cloud cu capacitatea de a gestiona dispozitivele pe care este instalat software-ul, care se integrează cu consola serverului de management.

Soluția va asigura cel putin protecție pentru stații de lucru și servere cu următoarele SO Windows edițiile ulterioare:

- Windows 7 (32 de biți, 64 de biți; RTM și SP1);

- Windows 8 (32-bit, 64-bit);

- Windows 8.1 (32 biți, 64 biți), inclusiv suport pentru actualizare pentru aprilie 2014 (32 biți, 64 biți) și actualizare pentru august 2014 (32 biți, 64 biți);

- Windows 10 (32 de biți, 64 de biți; RTM, Actualizare noiembrie (2015) și asistență obligatorie pentru Anniversary Update, Creators Update, Fall Creators Update та Spring Creators Update);

- Windows Embedded Standard 7 (32-bit și 64-bit);

- Windows Embedded POSReady 7 (32-bit și 64-bit);

- Windows Embedded Enterprise 7 (32-bit și 64-bit);

- Windows Embedded 8 Standard (32-bit și 64-bit);

- Windows Embedded 8.1 Industry Pro (32-bit și 64-bit);

- Windows Embedded 8.1 Enterprise Enterprise (32-bit și 64-bit);

- Windows Embedded 8.1 Pro (32 de biți și 64 de biți).

Revizuiri ulterioare pentru Mac OS:

- Mac OS X 10.9, 10.10, 10.11, 10.12, macOS 10.13, 10.15, 10.15.7, Mac OS 11 (Big Sur);

• Sistem de operare Linux al edițiilor următoare:

- Debian 6.0.5 Squeeze; 32 de biți și 64 de biți;

- Debian GNU / Linux 7 pe 32 și 64 de biți;

- Debian GNU / Linux 8 pe 32 și 64 de biți;

- Fedora 16, 17; 32 de biți și 64 de biți;

- SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32-bit și 64-bit;

- SUSE Linux Enterprise Desktop (SLED) 12 - 12 SP3, 32-bit și 64-bit;

- Ubuntu 12.04, 14.04, 15.10, 16.04; 32 de biți și 64 de biți.

Suport de protecție pe sistemele de operare server:

Windows OS edițiile ulterioare:

- Windows Server 2008 (32-bit, 64-bit; R2, SP1 și SP2);

- Windows Essential Business Server 2008 (64 de biți);

- Windows Small Business Server 2011 (64 de biți);

- Windows Server 2012;

- Windows Server 2012 R2;

- Actualizare Windows Server 2012 R2 pentru aprilie 2014 și august 2014;

- Windows Server 2016.

- Windows Server 2019.

• Sistem de operare Linux al ediţiilor următoare:

- Amazon Linux;

- CentOS 6U3, 6U4, 6U5, 6U6, 7, 7U1, 7U2, 7U3, 7U4, 32-bit şi 64-bit;

- Oracle Enterprise Linux (OEL) 6U2, 6U4, 6U5, 7, 7U1, 7U2, 7U3, 32-bit şi 64-bit;

- Oracle Linux Server 6U4, 6U5, 7, 7U1, 7U2, 7U3, 32-bit şi 64-bit;

- Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7-7U4, 32-bit şi 64-bit;

- SUSE Linux Enterprise Server (SLES) 11SP1 - 11SP3, 12, 12SP1, 32-bit şi 64-bit.

Un singur client pentru sistemele de operare Windows client şi server

Posibilitatea de instalare şi operare completă pe un computer cu un volum RAM de 1024 MB sau mai mult (pentru sistemul de operare Windows client şi sistemul de operare Linux

Suport pentru cloud şi medii virtuale în care este posibilă instalarea unui instrument de management centralizat, inclusiv componentele necesare ale unui astfel de instrument (bază de date, pluginuri de monitorizare, administrare, integrare etc.):

Amazon WorkSpaces;

- VMware WS 5.0 (staţie de lucru) sau o versiune ulterioară;
- VMware GSX 3.2 (enterprise) sau o versiune ulterioară;
- VMware ESX 2.5 (staţie de lucru) sau o versiune ulterioară;
- VMware ESXi 4.1 - 6.7 (inclusiv Actualizarea 1-2);
- Microsoft Virtual Server 2005;
- Windows Server 2008 Hyper-V;
- Windows Server 2012 Hyper-V;
- Windows Server 2012 R2 Hyper-V;
- Citrix XenServer 5 sau o versiune ulterioară;
- Virtual Box, furnizat de Oracle

Disponibilitatea de instrumente şi tehnologii pentru loadbalancing pentru distribuiriea sarcinii pe reţeaua de transmisie a datelor în procesul de schimb de date între clienţi şi serverul de custozi (sau servere)

Instrumente încorporate pentru acţiuni de audit atât pe partea computerelor personale client, cât şi pe serverul de control, cu posibilitatea de a exporta în continuare date de audit către sisteme şi fişiere externe

Prezenţa unui mediu de stocare separat pentru (bază de date sau baze de date) pentru stocarea parametrilor staţiilor de lucru finale şi ale serverului de gestionare, setările acestora, jurnalele de audit şi altele asemenea. Capacitatea de a face backup şi de a restaura mediul de stocare adecvat, dacă este necesar, atât manual, cât şi automat.

Prezenţa unui instrument de gestionare a licenţelor încorporate (licenţe) cu posibilitatea activării centralizate a tuturor funcţionalităţilor software pentru a proteja punctele finale cu licenţa (licenţele) corespunzătoare. Opţiunea de a activa (sau dezactiva) manual licenţa (licenţele) la fiecare punct final nu este permisă.

Disponibilitatea unui instrument pentru livrarea actualizărilor la semnăturile bazelor de date antivirus, setări (politici) etc.

Producătorul trebuie sa dispuna de seturi de instrucţiuni pentru instalare şi administrare în limbile minim engleza, rusă.

Producătorul trebuie sa dispuna de instrucţiuni pentru instalare şi administrare în limbile minim. engleza, rusă.

Disponibilitatea unor instrumente gratuite suplimentare (sau funcţionalitate încorporată) cu astfel de funcţionalităţi:

- instrumentatiu care permite trimiterea în mod automat a pachetelor de date cu mostre de fişiere infectate de la calculatoarele client în carantină centrală fără acces direct la calculatorul client în sine
- instrumentatiu care permite o curăţare completă a sistemului computerului client de software pentru a proteja acestea în caz de stergere nereuşită de către instrumentele standard ale sistemului de operare;
- instrumentatiu care permite gestionarea şi monitorizarea furnizorilor de actualizări în infrastructură bazat pe software de protecţie a punctelor finale;

- instrumentatiu care vă permite să obțineți informații extinse despre dispozitive externe și anume: informații despre producător, model, număr de serie;
- instrumentatiu care vă permite să integrați, prin API-uri deschise, un server centralizat pentru gestionarea parametrilor și setărilor de protecție împotriva amenințărilor pe stațiile de lucru client cu aplicații (sisteme) de monitorizare și gestionare la distanță (RMM) (sisteme de monitorizare și gestionare la distanță (RMM))
- instrumentatiu pentru furnizarea de date analitice avansate bazate pe baza de date a serverului pentru gestionarea setărilor de protecție împotriva amenințărilor și a setărilor de pe stațiile de lucru client, inclusiv în formă grafică;
- instrumentatiu pentru citirea simplificată a meniurilor și casetelor de dialog de pe server pentru gestionarea setărilor de protecție împotriva amenințărilor și a setărilor de pe stațiile de lucru ale clienților pentru persoanele cu dizabilități;
- instrumentatiu pentru extragerea și restaurarea fișierelor din mediul local de carantină dacă fișierul a fost pus în carantină din greșeală;
- instrumentatiu pentru actualizarea automată a parametrilor de comunicație între computerele client și serverul de control în cazul încetării unei astfel de comunicări din cauza mutării clientului către un alt domeniu, mutarea serverului de control și altele asemenea;
- instrumentatiu pentru diagnosticarea avansată a problemelor, care colectează date și detectează problemele obișnuite pentru continuarea ascensiunii către asistența producătorului
- instrumentatiu pentru diagnosticarea bazei de date a serverului de management.

Cerințe tehnice funcționale minim solicitate

Capacitatea de a gestiona centralizat protecția antivirus pe toate computerele client, indiferent de sistemul de operare utilizat pe acestea (în conformitate cu lista de sisteme de operare acceptate).

Suportă gestionarea centralizată utilizând un server de management dedicat, cu posibilitatea de a vă conecta la panoul de control al serverului utilizând un browser web.

Suportă gestionarea centralizată utilizând un server de management dedicat, cu posibilitatea de a se conecta la serverul de adiministrare utilizând consola de Manager Client

Serverul de management trebuie sa fie instalat pe sistemul de operare Windows Server.

Prezența unui agent de protecție pentru stațiile de lucru.

Posibilitatea de a instala de la distanță agenții pe stațiile de lucru cu sistemele de operare Windows într-un mod nesupravegheat (fără nicio acțiune a utilizatorilor).

Posibilitatea de a instala de la distanță agenți pe stațiile de lucru cu sistemele de operare Windows într-un mod nesupravegheat folosind următoarele produse terțe:

- Microsoft Systems Management Server;
- IBM Tivoli;
- Novell ZENworks.

Disponibilitatea tehnologiei de protectie a setările politicilor (regulilor) de securitate împotriva modificărilor neautorizate ale setărilor de către utilizatorii.

Posibilitatea configurării astfel de protecții cu o parolă.
Posibilitatea de auto-creare a pachetelor de instalare (instalatori) cu parametrii necesari (inclusiv module de protecție) pentru stațiile de lucru.

Capacitatea de utilizare ca mediu de stocare a unei bazei de date MS SQL pentru serverului de management.

Capacitatea de a construi o structură ierarhică de administrare de pe mai multe servere, atât pe un singur site, cât și situate în rețele diferite și geografic la distanță.

Atunci când serverele sunt distribuite in rețele diferite și la distanță geografică, este necesar să existe o tehnologie încorporată de replicare a datelor între astfel de servere, în timp ce replicarea trebuie să fie acceptată atât în modurile manuale, cât și în cele automate.

Abilitatea de a elimina automat sau de a migra obiecte infectate sau suspecte într-un mediu special de carantină.

Posibilitatea de scanare anti-virus pe calculatoarele client cu cerința de utilizator sau administrator, în modul manual

Prezența tehnologiei incorporate în antivirus care vă permite să excludeți de la scanarea fișierelor incluse în imaginea standard a unei mașini virtuale, care sunt utilizate pentru a clona (a crea noi) mașini virtuale;

Tehnologie de accelerare a scanării care vă permite să depășiți scanările programate și manuale ale fișierelor care au fost deja scanate de alte computere client din aceeași rețea.

Actualizarea manuală sau la timp a bazelor de date antivirus, a regulilor (politicilor). Abilitatea de a aplica reguli de actualizare diferite pentru diferite grupuri de clienți.

Capacitatea de a defini parametrii detaliați ai scanerului antivirus, precum: definirea obiectelor și metodele de scanare, capacitatea de a seta dimensiunea și timpul maxim pentru scanarea unui fișier, adâncimea maximă de pastrare a arhivelor și crearea de excepții;

Abilitatea de a reveni la versiunile anterioare ale bazelor de date de semnături.

Posibilitatea de a primi actualizări de baze de date de viruși din surse de rezervă dacă sursa principală de actualizare nu este disponibilă.

Capacitatea de a actualiza bazele de date antivirus atât de pe serverul de control, cât și direct de la serviciul producătorului de software pentru protejarea stațiile de lucru.

Abilitatea de a utiliza ca surse intermediare de actualizări și distribuirea politicilor și setărilor oricărui computer client ca furnizor de actualizări pentru un grup de clienți specificați.

Capacitatea de a primi actualizări pentru semnăturile de viruși și politicile clientului prin mijloace alternative (instrumente terțe) prin rețeaua locală de date (IBM Tivoli, Microsoft SMS etc.).

Disponibilitatea instrumentelor pentru identificarea computerelor client neprotejate (care nu au software pentru a proteja locurile de muncă finale).

Este necesar un sistem modular de protecție pe mai multe niveluri cu următorii parametri:

- protecție la nivel de rețea (firewall)
- protecție împotriva intruziunii (IPS)
- protecție la nivel de sistem de fișiere;
- protecție bazată pe reputația fișierelor;
- protecție bazată pe comportamentul proceselor generate de programe;
- un instrument pentru repararea și restaurarea sistemului de operare, dacă acesta este deja infectat.

Capacitatea obligatorie de a se integra cu sistemele de securitate a perimetrului rețelei folosind API-uri.

Capacitatea de a se integra cu sisteme de securitate perimetrale de rețea bazate pe cloud de la același producător.

Posibilitatea de integrare cu produsul * de la același producător, care permite efectuarea unei protecții extinse complexe, monitorizare și analiză împotriva amenințărilor de toate tipurile la toate nivelurile de infrastructură (lucrări finale, rețele locale și web și servere de poștă).

* Notă: acest produs trebuie să aibă:

- sandbox încorporat și cloud pentru analiza amenințărilor;
- căutarea și identificarea amenințărilor de zi „zero”, a atacurilor de hash;
- capacitatea de a exporta date către soluții SIEM terțe;
- un instrument de vizualizare pentru indicatorii de protecție (Indicatori de compromis - IoC), incluzând o reprezentare grafică completă a interacțiunii dintre aceștia (de exemplu, un lanț din forma „fișiere implicate în atac” - „adrese IP din care au fost descărcate fișierele” - „utilizatori afectați de atacuri "-" calea distribuției către alți utilizatori "etc.);
- să fie capabil să blocheze linkurile malicioase din e-mailuri în etapa de livrare a scrisorii către utilizator.

Existența unui mecanism de detectare a conformității sau a neconformității cu criteriile specificate pentru prezența corecțiilor de securitate (patch-uri) în sistemul de securitate al sistemului de operare la stațiile de lucru.

Disponibilitatea tehnologiei permite reducerea volumului de semnături antivirus stocate pe stațiile de lucru client de cel puțin două ori, prin studierea reputației fișierelor prin mediul cloud existent al producătorului. Atunci când examinați reputația unui fișier, numai detaliile fișierului, cum ar fi dimensiunea acestuia, data creării, hash etc., ar trebui transferate în cloud, nu fișierul în sine.

Cerințe de protecție:
Disponibilitate de protecție împotriva: rootkit-uri, programe malware, spyware, troieni, adware, criptare, software potențial nedorit și periculos, atacuri de rețea și spam. Suport pentru această protecție atât pentru PC-uri fizice, cât și pentru medii virtuale (VDI, sesiuni de terminal etc.).
Posibilitatea de a crea excepții pentru a căuta amenințări (viruși) ale următoarelor elemente ale sistemului de operare Windows: fisier; • catalog; • amenințări cunoscute; • extensie de fișier; • domeniu; • anexă.
Disponibilitatea protecției împotriva atacurilor și amenințărilor care se răspândesc prin rețelele web și locale, serviciile de e-mail, mass-media amovibilă, inclusiv: • protecție împotriva amenințărilor precum „botnet”; • protecție împotriva falsificării IP și MAC; • protecție împotriva amenințărilor de zi „zero”; • protecție împotriva amenințărilor care pot exploata vulnerabilitățile în Java, Flash și alte aplicații; • protecție împotriva amenințărilor mascate în pachete (de exemplu, arhive de instalare).
Suport pentru tehnologia anti-exploit în memoria computerului bazată pe tehnologii de vulnerabilitate cunoscute: • prevenirea executării codului JAVA în afara sandbox-ului, inclusiv - dezactivarea Managerului de securitate JAVA • Prevenirea suprascrierii cadrelor Structured Exception Handler (SHE) în memoria computerului pentru a intercepta handlerul SEH în Windows; • Prevenirea executării programelor (aplicațiilor) care pot provoca depășirea spațiului de adrese („heap”) în memoria computerului.
Asigurarea protecției în timp real.
Pentru stațiile de lucru cu sistemele de operare Windows, este necesar disponibilitate unui mecanism de scanare a fișierelor în timp real cu analiza simultana pe baza analizei euristice, a învățării automate și a datelor de reputație. Acest motor de scanare ar trebui să poată adăuga codul său la aplicațiile care rulează exclusiv în modul utilizator Windows (UMH) pentru a analiza comportamentul acestei aplicații și a o închide imediat în caz de activitate rău intenționată.
Suport pentru scanarea antivirus a mediilor amovibile în modul automat și manual.
Este obligatoriu să dispuna de un driver special pentru pornirea timpurie a sistemului ELAM, care protejează computerele client în timpul startarii
Posibilitatea de a scana fișiere la pornirea sistemului (inclusiv sectorul de boot, RAM), în timpul operațiilor de fișiere, în modul manual și în timp.
Tehnologie încorporată care monitorizează aplicațiile și fișierele care încearcă să modifice setările DNS (inclusiv fișierul gazdă de pe computerul client).
Abilitatea de a verifica conținutul arhivelor cu posibilitatea de a regla profunzimea unei astfel de verificări.
Existența modulului de protecție împotriva spamului și a altor amenințări cu posibilitatea integrării în clientul de poștă electronică. Posibilitatea de a instala agentul pe o stație de lucru cu sau fără modul curent (pentru punctele finale care nu utilizează clienți de e-mail).
Verificarea traficului HTTP, FTP, POP, SMTP, IMAP, inclusiv a canalelor de transmisie de date criptate.
Prezența unui firewall personal, care conține un master pentru crearea reguli și editor pentru zonele de rețea cu posibilitatea de a crea diferite profiluri pentru un firewall personal, care poate fi comutat automat în funcție de condițiile de utilizare ale stațiilor de lucru (la care rețea este conectat stația de lucru, prin care interfață este conectat stația de lucru și etc.).
Abilitatea de a restricționa accesul la anumite categorii de site-uri pe baza regulilor firewall în conformitate cu

următoarele criterii:

- o aplicație care utilizează accesul la Internet;
- protocol utilizat;
- adaptorul de rețea utilizat.

În același timp, restricționarea accesului la anumite categorii de site-uri ar trebui setată atât de adresa IP, cât și de numele DNS al domeniului sau gazdei.

Sistem de detectare și prevenire a intruziunilor (IDS sau IPS) care protejează computerul de malware și de activități nedorite.

Capacitatea de a detecta și preveni intruziunile (cu blocarea descărcării și executării obiectelor rău intenționate) la diferite niveluri ale modelului de rețea OSI (de la rețeaua [2] la aplicația [al șaptelea] strat) pentru Windows.

Capacitate obligatorie de a vă crea propriile semnături pentru sistemul de prevenire a intruziunilor.

Capacitatea de a exclude anumite stații de lucru de la scanarea de către sistemul de detectare și prevenire a intruziunilor și o astfel de excludere trebuie setată în conformitate cu următoarele criterii: adresă IP, interval de adrese IP sau mască de subrețea.

Prezența unor tehnologii care permit analizarea fișierelor în vederea reputației și emiterea unui verdict asupra prejudiciului sau siguranței acestora. Tehnologia bazată pe reputație ar trebui să se bazeze pe informații localizate și analizate constant în mediul cloud al producătorului.

Notă: reputația reprezintă informații despre câte computere din lume este prezent acest fișier, cât timp a existat, prin ce canale de comunicare și din ce resursă a fost primit și cu ce resurse interacționează etc.

Disponibilitatea propiei tehnologiei (instrumentariu) implementat efectiv pentru controlul și gestionarea autorizațiilor pentru:

- lansarea aplicațiilor predefinite;
- accesul sau încetarea proceselor specificate;
- acces la fișiere, chei de registry și biblioteci din aplicații specificate.

Această tehnologie ar trebui să poată crea propriile reguli în conformitate cu următoarele criterii:

- suport pentru sistemul de operare Windows și browserele EI, Egde, Firefox;
- posibilitatea de a folosi măști de substituție (simboluri „*”, „?” etc.);
- capacitatea de a specifica unde ar trebui să funcționeze aceste reguli (unități locale, unități de rețea, suporturi amovibile etc.);
- capacitatea de a stabili condiții pentru diferite tipuri de operațiuni de intrare-ieșire (citire, scriere, modificare etc.);
- capacitatea de a crea excepții.

Tehnologia proprietară (instrument) pentru controlul și gestionarea permisiunilor pentru a rula aplicații și pentru a accesa fișiere și procese trebuie să fie integrată în software-ul de protecție a punctelor finale (să fie o parte integrantă a produsului).

Posibilitatea de a bloca software-ul cu:
- „liste albe” bazate pe amprente „digitale” folosind tehnologia de calcul sumă hash (adică liste de aplicații care pot rula, în timp ce orice alte programe nu vor fi disponibile pentru a rula)
- “liste negre” bazate pe amprente digitale folosind tehnologia de calcul sumă hash (adică liste de aplicații care nu vor putea rula, în timp ce orice alte programe vor fi disponibile pentru a rula).

Disponibilitatea propriei tehnologiei incorporate efficiente pentru controlul suporturilor amovibile cu capacitatea de a crea reguli pentru:

- tipul dispozitivului;
- producătorul dispozitivului;
- modelul și numărul de serie al dispozitivului.

Disponibilitatea propriei tehnologiei incorporate efficiente pentru controlul suporturilor amovibile ar trebui să fie integrată în software-ul de protecție a punctelor finale (să fie o parte integrantă a produsului).

Posibilitatea de a căuta în Windows după ID-ul clasei sau ID-ul dispozitivului în funcție de șabloane (folosind asteriscul „*”).

Capacitatea de a căuta în MacOS prin expresii regulate care pot utiliza caractere:

- . (Punct)
- \ (backslash)
- [set], [^ Set] (set)
- * (asteriscuri)
- + (plus).

Disponibilitatea propriei tehnologiei incorporate efficiente pentru instalarea forțată centralizată a actualizărilor de securitate (inclusiv patch-uri Windows Update) pe stații de lucru cu sistem de operare Windows.

Disponibilitatea propriei tehnologii incorporate efficiente pentru blocarea fișierelor după numele sau extensia specificată.

Cerințe de administrare și audit:

Disponibilitatea managerului de utilizatori, care vă permite să creați utilizatori diferiți ai serverului de administrare (administratori, operatori etc.) și să le atribuiți diferiți drepturi de acces la partiții individuale, grupuri de computere de pe serverul de administrare.

Abilitatea de a controla de la distanță serverul de administrare folosind un browser web cu posibilitatea de a furniza astfel acces la adrese IP specifice ale utilizatorilor.

Prezența unei reviste în care:

- toate modificările în configurație și toate acțiunile efectuate de utilizatorii serverului de administrare sunt monitorizate și înregistrate;
- Urmărirea evenimentelor legate de acțiuni pe stații de lucru.
- Urmărirea evenimentelor legate de activitatea rootkiturilor, malware, spyware, troieni, adware, software criptat, potențial nedorit și periculos, atacuri de rețea și spam, etc.

Posibilitatea de a crea evenimente personalizate cu jurnalizare și mesaje suplimentare prin e-mail către persoane responsabile.

Posibilitatea de a salva jurnalele pe stațiile de lucru pentru analize suplimentare sau tipărirea unui astfel de jurnal.

Prezența funcționalității încorporate în serverul de gestionare care vă permite să setați volumul (dimensiunea) și parametrii de stocare a jurnalelor la stațiile de lucru finale pentru evenimente de sistem, evenimente legate de amenințări, trafic de rețea

Prezența unui panou web, care face posibilă monitorizarea stării protecției antivirus a rețelei corporative în timp real și oferă informații actualizate despre starea de securitate.

Este imperative ca solutia sa dispuna de propriul serviciu web care vă permite să vizualizați jurnalele folosind browserele web în lunile de lucru la distanță.

Suport obligatoriu pentru un protocol criptat pentru astfel de acțiuni cu un port separat, care poate fi setat de administratorul de sistem în setările serverului de administrare.

Integrare cu Active Directory și / sau LDAP.

Suportă autentificarea factoriala dubla RSA SecurID pentru a proteja conturile de administrator

Prezența unui mecanism încorporat (instrumente) pentru crearea și restaurarea copiilor de rezervă ale serverului de administrare (inclusiv baza de date pe care rulează serverul).

Posibilitatea de a crea un fișier dedicat de recuperare de urgență (cu parole de criptare, ID de domeniu al fișierelor de depozitare de chei, fișiere de certificate, licențe etc.).

Abilitatea de a crea diferite grupuri de utilizatori cu parametri (diferiți) separați (reguli, module de securitate etc.). Abilitatea de a aplica politici ca pentru toți utilizatorii simultan și pentru grupuri individuale.

Disponibilitatea instrumentelor pentru editarea grupurilor de utilizatori, care permite:

- crearea, editarea,ștergerea grupuri de utilizatori;
- importarea grupuri din Active Directory și crearea un arbore similar de grupuri;
- efectuarea sincronizării periodică a grupurilor configurate cu Active Directory.

Capacitatea de a crea politici separate pentru fiecare tip de protecție (protecție antivirus, firewall, IPS etc.).

Abilitatea de a exporta / importa politici într-un fișier separat

Capacitatea de a construi un set de pachete de instalare pentru instalarea lor ulterioară pe stații de lucru, inclusiv pachete pentru diverse sisteme de operare, diverse versiuni de software pentru protejarea locurilor de muncă finale.

Posibilitatea instalării centralizate a agenților pe stații de lucru (inclusiv un grup de stații) utilizând tehnologia „push”. Posibilitatea de a trimite un link către locația pachetelor de instalare prin e-mail în scopul instalării manuale a pachetului pe locurilor de muncă finale.
Posibilitatea aplicării centralizate a politicilor pe stații de lucru atât pentru stații în ansamblu, cât și pentru utilizatorii săi individuali.
Abilitatea de a activa și dezactiva de la distanță module de protecție precum firewall personal, protecție în timp real, protecție client e-mail, protecție acces internet, control web și multe altele
Capacitatea de a rula de la distanță pe stații de lucru proceduri legate de protecția punctelor finale, cum ar fi scanarea, actualizarea politicilor și altele asemenea.
Disponibilitatea instrumentelor pentru configurarea programului pentru actualizările de semnături și politici ale software-ului antivirus pe stații de lucru. Având un instrument pentru a identifica mașinile virtuale invitate care au un agent software de protecție a punctelor finale instalat ca clienți temporari. Prezența unor astfel de oportunități este obligatorie: • stabilirea perioadei de îmbătrânire pentru astfel de mașini virtuale; • eliminarea automată a agenților pe astfel de mașini virtuale (marcată ca temporară) odată cu eliberarea simultană a licenței după o perioadă de îmbătrânire specificată.
Cerințe de termen de utilizare, asistență și cumpărare:
Întregul volum al software-ului trebuie să fie furnizat pe un termen nu mai mic de 12 (douăsprezece) luni cu suport tehnic și mentenanță de la producător pentru aceiași perioadă de cel puțin 12 (doisprezece) luni., pentru minimum 700 stații lucrătoare, servere și mașini virtuale.
Dreptul de a utiliza software-ul propus trebuie să fie disponibil pe bază de utilizare temporară (cel puțin 12 luni).
Disponibilitatea de asistență tehnică de la producătorul de software antivirus.
Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local din partea partenerului;
Producătorul trebuie sa confirme autorizarea partenerului vis-a-vis de dreptul de vânzare a produselor pe teritoriul Republicii Moldova (copia certificatului de partener autorizat)

ANEXA nr. 2
la LOTUL II. „Sistem monitorizare a echipamentelor TI”

Sistem de monitorizare a infrastructurii TI

Specificația articolului	Cerințe privind specificațiile produsului
Funcționalitatea software-ului de sistem	
Termeni de utilizare	Licența se acordă pe un termen de minim 12 luni, care include suport și mentenanță pentru aceiași perioadă de minimum 12 luni, pentru peste 800 de stații de lucru, servere, mașini virtuale, echipamente de rețea și periferice.
Criterii și cerințe generale pentru sistemul de monitorizare	• monitorizarea, analiza și controlul performanței următoarelor componente TI: echipamente de rețea, echipamente de stocare a datelor, servere, aplicații, infrastructură de virtualizare, sisteme de operare, baze de date; • monitorizarea, analiza și controlul performanței echipamentelor și software-ului de la diferiți producători folosint protocoale standarde de monitorizare; • monitorizarea și analiza lucrărilor, cererilor, cozilor de citire / scriere pentru baze de date ale diferiților producători; • monitorizarea, analiza și controlul performanței și disponibilității hard diskurilor și sistemelor de stocare a datelor de la diferiți producători; • monitorizarea, analiza și controlul performanței și disponibilității site-urilor web; • monitorizarea, analiza și controlul performanței și stării platformelor de virtualizare; • monitorizarea infrastructurii Active Directory; • îmbunătățirea eficienței operaționale și accelerarea identificării problemelor în funcționarea infrastructurii TI, soluția utilizând tablouri de bord preinstalate și configurate, sisteme de notificare și raportare încorporate; • îmbunătățirea nivelurilor de servicii și reducerea timpului de nefuncționare pentru sisteme și servicii, asigurarea disponibilității și productivității acestora; • gestionarea tuturor componentelor dintr-o console, într-o singură platformă; • sistemul trebuie să fie un instrument pentru monitorizarea operațională a echipamentelor și serviciilor, să aibă o interfață grafică și un set de instrumente care să permită înregistrarea și analiza evenimentelor care au loc în infrastructura TI. • detectarea automată a obiectelor infrastructurii TI; • scanarea automată a rețelei, inclusiv identificarea dispozitivelor de rețea, automatizarea proceselor cu instrumente și script-uri;
Protocoale și standarde susținute	Sistemul trebuie să accepte și să susțină următoarele protocoale: • SNMP v1 / v2 / v3; • SNMP trap; • Syslog; • ICMP; • SSH; • WMI; • SMI-S.

Monitorizarea și controlul performanței echipamentelor de rețea	• control automat al următoarelor elemente: o routere; o comutatoare; o firewall-uri; o dispozitive wireless; • descoperirea automată a dispozitivelor din rețea cu capacități SNMP și ICMP: o intervale de adrese IP; o subrețele; o adrese IP separate; o Active Directory. • oferirea statisticilor detaliate în timp real ale performanței aplicației după detectare și / sau reglare: o încărcare procesor; o folosirea memoriei; o utilizarea interfeței de rețea; o pierderea pachetelor. • detectare și control dispozitive IPv4 și IPv6; • monitorizarea componentelor individuale ale sistemului de echilibrare a sarcinii; • identificarea și clasificarea a cel puțin 1200 de aplicații în mod implicit; • import automat de dispozitive detectate; • monitorizarea echipamentelor și a rețelelor fără fir (wireless, Wi-Fi) și a clienților acestora; • detectarea și depanarea căilor de rețea pentru o anumită comunicație TCP locală; • susținerea dispozitivelor care utilizează protocoale SNMP v1, v2, v3, SNMP trap, WMI; • afișarea valorilor de volum agregate pentru fiecare aplicație / nod; • urmărirea componentelor individuale în firewall, inclusiv: numărul de conexiuni, tuneluri VPN de la site la site și de la distanță, identitatea și utilizarea interfeței, starea de disponibilitate ridicată și starea de sincronizare a configurației; • crearea de rapoarte privind funcționarea comutatoarelor virtualizate; • disponibilitatea versiunii mobile a consolei pentru vizualizarea imediată de către administratori; • disponibilitatea parametrilor pentru automatizarea și planificarea procesului de detectare; • determinarea disponibilității unui dispozitiv folosind doar SNMP; • posibilitatea de a indica perioada de stocare a datelor; • posibilitatea creării hărților topologice; • urmărirea stării echipamentelor furnizorilor populari precum Cisco, DELL, F5, Juniper, HP etc., precum și furnizarea de alerte și rapoarte privind starea echipamentelor monitorizate; • afișarea în consola web a notificărilor despre descoperirea de noi dispozitive în rețea; • afișarea datelor atât în timp real, cât și retrospectiv sub formă de diagrame cu alegerea timpului; • afișarea următoarelor informații: Alerte pentru protocoale de rutare majore (BGP, OSPF, RIP, EIGRP) cu căutare tabel de rutare și opțiuni de căutare, inclusiv VRF, modificări implicite ale rutei, rutare de redirecționare, topologie de rutare și stări vecine; • evidențierea cu diferite culori a dispozitivului în dependență de

	starea sa și starea interfeței. Afișarea avertizărilor și a stării critice • afișarea următoarelor statistici: lățimea de bandă a interfeței, traficul curent (bps), numărul total de octeți primiți / trimiși etc; • filtrarea interfețelor descoperite pentru a exclude interfețele virtuale și porturile de acces și selectarea interfeței pe baza șabloanelor; • monitorizarea traficului multicast, alerte de topologie, rute multicast, erori multicast etc; • interzicerea adăugării de dispozitive cu mai multe adrese IP ca dispozitive redundante și furnizarea unei liste cu toate adresele IP cunoscute pentru un dispozitiv.
Monitorizarea și controlul performanțelor serverelor, sistemelor de operare și aplicațiilor	• scanarea rețelei și detectarea automata a serverelor și a aplicațiilor care rulează pe ele; • furnizarea automată în timp real a proceselor sistemului și statistici detaliate privind performanța aplicației după detectarea și configurarea acesteia; • asigurarea colectării informațiilor despre: o starea aplicației; o numărul de utilizatori; o servicii și procese; o funcționarea sistemului de operare; o echipament. • furnizarea de informații despre hardware-ul serverelor de la producători renumiți (IBM, HP, DELL, Fujitsu), dar fără a se limita la: o unități centrale de procesare; o memorie; o starea ventilatoarelor; o starea surselor de alimentare. • detectarea și monitorizarea automată a echipamentelor noi descoperite; • monitorizarea în timp real a jurnalelor de evenimente Windows, inclusiv categoria evenimentului, ID-ul evenimentului și sursa; • sistemul trebuie să permită folosirea scripturilor personalizate VBscript, Perl, PowerShell etc; • sistemul trebuie să permită crearea șabloanelor de monitorizare personalizat al unei aplicații către toate celelalte servere pe care este implementată această aplicație; • o asociere a parametrilor importanți într-un singur șablon de monitorizare care poate fi aplicat într-un șablon aplicațiilor implementate pe diferite servere; • disponibilitatea versiunii mobile a consolei pentru vizualizarea imediată de către administratori; • disponibilitatea monitorizării prin WMI sau SNMP, monitoare de contor de performanță, monitoare WMI, monitoare de contor de performanță VMware etc; • disponibilitatea parametrilor să monitorizeze interfața utilizatorului pentru diverse aplicații și servicii, precum HTTP, FTP, DHCP, DNS, SQL Server, Oracle, JSON etc., pentru detectarea timpurie a problemei; • disponibilitatea parametrilor pentru a indica perioadele de păstrare a datelor; • disponibilitatea metodelor de monitorizare expertă care arată starea și performanța parametrilor cheie (servicii, lungimea cozii pentru Exchange, interogări SQL pentru baze de date etc.) pe baza

	celor mai bune practici și experiență operațională; • sistemul trebuie să permită: o înregistrarea evenimentelor de audit ale utilizatorilor; o înregistrarea proceselor stopate; o înregistrarea serviciilor oprite / pornite / repornite; o înregistrarea nodurilor repornite; • detectare dependențe de aplicații și conexiuni între serverele de aplicații, precum și monitorizarea informațiilor despre conexiunile de intrare și ieșire la nivelul fiecărui proces; • monitorizarea continuă a serverelor web Microsoft IIS, inclusiv: o serviciu; o procese; o conexiuni la site-uri web individuale; o timp de raspuns; o grup de aplicații separat; o alte statistici precum cache și conexiuni. • Obținerea valorilor de performanță I/O pe disc pentru procese și servicii monitorizate prin WMI; • detectare JMX pentru monitorizarea aplicațiilor Java precum JBoss, Tomcat, WebLogic etc; • afișarea datelor atât în timp real, cât și retrospectiv sub formă de diagrame cu alegerea timpului; • evidențierea cu diferite culori a stării aplicației și stării serviciilor importante pentru a afișa avertismente și starea critică; • monitorizarea performanței aplicațiilor și a sistemelor de operare ale instanțelor din cloud;
Monitorizarea bazelor de date	• suport pentru monitorizarea următoarelor baze de date: o Microsoft SQL Server (toate versiunile); o Oracle SE și EE; o MySQL (toate versiunile); o MariaDB (toate versiunile); o PostgreSQL (toate versiunile). • monitorizarea următoarelor elemente ale Microsoft SQL server: o jurnal de erori SQL; o informații despre baze de date individuale; o starea agentului SQL; o indexuri fragmentate; o numărul de conexiuni. o cozi de așteptare; o utilizatori. • analiza cauzelor problemelor prin maparea instrucțiunilor SQL, contextului, valorilor de performanță, latenței și timpilor de răspuns și recomandărilor de optimizare a performanței; • afișarea informațiilor într-un singur tablou de bord; • furnizarea de recomandări pentru reglarea tabelelor prin corelarea informațiilor despre interogări ineficiente, structura tabelului, recomandări de index și planuri de execuție; • monitorizarea proactivă a bazei de date, starea sistemului și identificarea tendințelor negative înainte de apariția problemelor; • sistemul de monitorizare nu trebuie să mărească încărcătura asupra sistemului de gestiune a bazei de date mai mult de 1%; • suport pentru implementarea fără agent; • descrierea cauzelor evenimentelor de așteptare pentru o înțelegere mai detaliată a motivelor pentru timpul de răspuns SQL lung; • furnizarea instrumentelor pentru a analiza și optimiza performanța

	pe baza interogărilor, sesiunilor, serverelor și sistemelor de stocare; • identificarea problemelor de performanță care afectează cel mai mult timpul de răspuns al utilizatorului final; • afișează o vedere detaliată a performanței stocării, inclusiv latența și I/O, atât în timp real, cât și în retrospectivă; • monitorizarea stării MS SQL Availability Group, inclusiv replicarea și starea bazei de date; • suport pentru planurile de adaptare Oracle.
Monitorizarea sistemelor de stocare a datelor	• monitorizarea performanței și capacității infrastructurii de stocare fizică și virtuală; • descoperirea automată a dispozitivelor din rețea cu capacități SMI-S la introducerea: o intervale de adrese IP; o adrese IP separate. • afișarea statisticilor detaliate de performanță în timp real după descoperirea / configurarea dispozitivului: o performanța controlerului; o performanța LUN; o performanța hard disk-urilor. o numărul total de operații I/O pe secundă; o timpul de serviciu; o timp de răspuns I/O; o lungimea cozii de așteptare. • monitorizarea ratei de creștere a volumelor de stocare și prognozarea insuficienței spațiunui de stocare; • izolatie hotspoturi de stocare și surse de conflict; • afișarea informațiilor capacitate, alocare, utilizare și prognoză la toate nivelurile mediului de stocare (raw, RAID, LUN, stocare date și sistem de fișiere); • monitorizarea comutatoarelor Fibre Channel de la producătorii populari pentru informații despre infrastructura SAN; • evidențierea cu diferite culori a stării dispozitivului pentru a afișa avertizări și stări critice; • afișarea datelor atât în timp real, cât și retrospectiv, sub formă de diagrame cu alegerea timpului; • disponibilitatea parametrilor pentru a indica perioadele de păstrare a datelor;
Monitorizarea și gestionarea sistemelor de virtualizare	• gestionarea cu un singur panou a hipervizoarelor eterogene, cum ar fi VMware vSphere și Microsoft Hyper-V; • Monitorizarea performanței VMware, inclusiv VMware ESX, vSphere, ESXi, vCenter Server; • colectarea de informații despre performanța și capacitatea VMware vSAN; • colecție de informații despre performanța și capacitatea clusterelor, gazdelor și mașinilor virtuale din Hyper-V; • monitorizarea performanțelor și evidențierea problemelor I/O de stocare; • monitorizarea, detectarea și eliminarea blocajelor lățimii de bandă ale platformelor de virtualizare; • determinarea plasării optime a mașinilor virtuale; • oferirea de asistență în planificarea achizițiilor noi, identificarea resurselor suprautilizate și subutilizate; • identificarea mașinilor virtuale inactive, învechite, detectarea fișierelor pierdute și a mașinilor virtuale supraîncărcate;

	• monitorizarea configurației mașinilor și gazdelor virtuale, precum și afișarea dinamică a modificărilor de configurație; • oferirea anticipată a recomandărilor pentru creșterea resurselor (CPU, RAM, Storage, Networking) pe baza tendințelor și modelelor istorice. • generarea de rapoarte cu statistici detaliate de utilizare care acoperă consumul de resurse proiectat și recomandări pentru satisfacerea nevoilor viitoare; • implementarea promptă sau planificată a acțiunilor de remediere oferite de recomandările automate; • detectarea și monitorizarea automată a noilor instanțe;
Specificații pentru interfața de gestionare	Sistemul trebuie să ofere următoarele funcționalități: • interfață grafică de utilizator de înaltă calitate cu actualizări de informații asincrone; • setarea parametrilor pentru adăugarea / eliminarea secțiunilor paginilor web; • acordarea acces la utilizator / operator prin intermediul consolei web cu următoarele caracteristici: o consola web trebuie să fie accesibilă atât central, cât și de la distanță; o consola web trebuie să fie accesibilă prin intermediul browserelor standard; o consola web trebuie să fie ușor de utilizat cu detaliile informațiilor solicitate; o Consola web trebuie să poată crea tablouri de bord personalizate pentru o varietate de scopuri: performanță, programarea capacității, recuperarea încărcării și multe altele. o Consola web trebuie să se poată integra cu Active Directory pentru ca utilizatorul să se conecteze la sistem; o Consola web trebuie să ofere posibilitatea de a crea un tablou de bord dinamic care să ofere vizibilitate profundă și corelație la diferite puncte de date istorice din diferite părți ale infrastructurii. Rezultatul trebuie exportat în format tabel; o consola web trebuie să ofere o singură vizualizare a alertelor și evenimentelor; o consola web trebuie să ofere o diagramă interactivă pentru noduri, interfețe, graficele de volum etc.; o Consola web trebuie să fie capabilă să se redimensioneze atunci când un număr mare de utilizatori sunt conectați în același timp o Consola web trebuie să fie capabilă de mai mulți utilizatori simultani și să accepte nu mai puțin de 25 de sesiuni de utilizatori simultane fără degraderea performanței; o Consola web trebuie să evidențieze rapid aplicațiile problematice bazate pe diferite proprietăți, cum ar fi aplicațiile care nu rulează, aplicațiile cu utilizare ridicată a procesorului, utilizarea memoriei etc. o Consola web trebuie să evidențieze rapid dispozitivele cu probleme pe baza diferitelor proprietăți, cum ar fi timpul de răspuns, utilizarea procesorului, utilizarea memoriei, utilizarea ridicată a interfeței etc. o Consola web trebuie să fie capabilă să se integreze pentru a reda automat obiecte de infrastructură virtuală relevante, cum ar fi depozite de date și obiecte de stocare; o Consola web trebuie să fie capabilă să se integreze pentru a

	reda automat aplicații relevante și obiecte de stocare, cum ar fi LUN-uri, cu obiecte de infrastructură virtuală corespunzătoare, cum ar fi depozite de date și clustere. o consola web trebuie să detecteze rapid dispozitivele cu probleme (de exemplu, cu un procent ridicat de porturi utilizate); o Consola web trebuie să detecteze dispozitivele cu probleme pe baza diferitelor proprietăți, cum ar fi Total IOPS, latență, citire și scriere; o consola web trebuie să accepte gruparea tranzacțiilor și / sau pașilor web; o Consola web trebuie să poată crea un tablou de bord personalizat și să restricționeze vizualizarea la utilizatori pe baza aplicațiilor, dispozitivelor sau interfețelor, adică să aibă acces bazat pe roluri. o consola web trebuie să poată exporta orice pagină web în format PDF; o consola web trebuie să ofere pe o singură pagină o vizualizare unificată a avertismentelor, întreruperilor hardware, evenimentelor; o Consola web trebuie să înregistreze acțiunile și evenimentele utilizatorilor pe consola web în scopuri de audit, cu acces ulterior la alerte și raportări; o consola web trebuie să prezinte rapid tranzacțiile web și pașii problemelor împreună cu instantaneele paginii.
Setări de alertă incident	• determinarea operațională și asigurarea informațiilor necesare pentru soluții, probleme de performanță cu sistemul de avertizare și recomandări: o sistemul de avertizare trebuie să poată lega dinamic statisticile și să seteze automat pragul de avertizare și pragul critic; o sistemul de avertizare trebuie să furnizeze alerte cu privire la o posibilă problemă cu baza de date în diferite categorii: latență, resurse, valori administrative și valori ale utilizatorilor; o sistemul de avertizare trebuie să suprime avertismentele în timpul întreținerii programate; o sistemul de avertizare trebuie să permită introducerea interogărilor SQL pentru a crea reguli de baze de date; o sistemul de avertizare trebuie să permită diverse acțiuni, dar nu se limitează la: trimiterea de e-mailuri, trimiterea de capcane SNMP, lansarea de fișiere executabile, trimiterea de mesaje SMS, redarea unui sunet, trimiterea prin e-mail a paginilor web etc.; o sistemul de avertizare trebuie să poată trimite notificări prin e-mail care nu necesită explicații suplimentare; o sistemul de avertizare trebuie să poată crea noi avertismente de la zero și reglați pragurile; o sistemul de avertizare trebuie să poată genera alerte pe baza informațiilor despre starea de muncă pe termen lung; o sistemul de avertizare trebuie să furnizeze informații despre avertismente și evenimente bazei de date pentru o utilizare ulterioară. • definirea condițiilor complexe; • gestionarea și afișarea evenimentelor și avertismentelor în consola web; • introducerea interogărilor personalizate pentru a crea reguli de

	baze de date.
Sistem de raportare a incidentelor în exploatarea echipamentelor și serviciilor	• acordarea rapoartelor gata făcute despre date statistice curente sau istorice pentru sistemul de raportare, care trebuie să genereze / creeze rapoarte utilizând consola web și să îndeplinească următoarele cerințe: o sistemul de raportare trebuie să fie capabil să genereze rapoarte statistice care să poată fi utilizate pentru planificarea viitoare și lucrările de depanare; o sistemul de raportare trebuie să poată grupa mai multe rapoarte într-un singur raport complex; o sistemul de raportare trebuie să fie capabil să plaseze diagrame și tabele într-un singur raport; o sistemul de raportare trebuie să ofere posibilitatea unei personalizări avansate, luând în considerare parametrii pentru introducerea interogărilor utilizatorilor direct sub forma unei interogări în baza de date; o sistemul de raportare trebuie să aibă un număr mare de reguli încorporate pentru utilizare imediată și personalizare; o sistemul de raportare trebuie să poată importa și exporta rapoarte create de alți utilizatori; o sistemul de raportare trebuie să personalizeze rapoartele prin adăugarea / eliminarea coloanelor, setarea filtrelor, specificarea intervalelor de timp, gruparea coloanelor etc; o sistemul de raportare trebuie să sprijine utilizarea unui program extern ca alertă; o sistemul de raportare trebuie accepte personalizarea condițiilor de notificare cu personalizarea canalelor de notificare; o sistemul de raportare trebuie să sprijine transmiterea mesajelor către sistemul de monitorizare NOC sau alte sisteme; o sistemul de raportare trebuie să accepte diverse formate: PDF, HTML și CSV; o sistemul de raportare trebuie să permită trimiterea prin e-mail a tablourilor de bord create în consola web. o sistemul de raportare trebuie să permită trimiterea rapoartelor într-un program: zilnic, săptămânal, lunar; o sistemul de raportare trebuie să ofere posibilitatea de a genera un raport bazat pe instrucțiuni SQL personalizate, inclusiv expirarea și intervalul de timp; o sistemul de raportare trebuie să ofere posibilitatea de a programa rapoarte pentru transmiterea automată ulterioară; o sistemul de raportare trebuie să sprijine crearea de rapoarte specifice de management și audit; o sistemul de raportare trebuie să furnizeze rapoarte de management al performanței care să conțină informații despre toate echipamentele; o sistemul de raportare trebuie să ofere opțiuni pentru salvarea rapoartelor personalizate cu acces suplimentar la acestea în consola web; o sistemul de raportare trebuie să furnizeze șabloane pentru crearea ușoară a rapoartelor privind funcționarea diverselor baze de date; o sistemul de raportare trebuie să furnizeze rapoarte detaliate privind accesul utilizatorilor în scopul respectării reglementărilor și în scopuri de audit.

Proprietățile obiectului informațional	• gruparea aplicațiilor după diferite proprietăți; • acordarea permisiunii de grupare a tranzacțiilor web și a etapelor tranzacției; • adăugarea de membri la grupuri din mers, specificarea unei proprietăți care poate modifica dinamic valorile, cum ar fi atingerea spațiului liber minim pe un volum; • definirea relației dintre servere și aplicații pentru a evita alerte false prin e-mail în caz de eșec; • maparea relației dintre resursele conectate de-a lungul timpului, dependențele dintre obiectele centrului de date virtuale, cum ar fi mașinile virtuale, gazdele, magazinele de date, clustere și vApp-uri; • disponibilitatea opțiunilor avansate de căutare, filtrarea și sortarea atributelor de configurație și performanță colectate.
Hărți topologice	Trebuie să existe cel puțin: • afișare grafică detaliată despre performanță și aplicație în timp real; • conexiune automată dispozitive care folosesc informații topologice colectate în timpul căutării și descoperirii, precum Cisco Discovery Protocol sau Link Layer Discovery Protocol; • capacitatea de a schimba fundalul, iconițele și hărțile cu posibilitatea de a le detalia; • afișarea utilizării canalului ca „hartă a vremii”; • afișarea localizării dispozitivelor la nivel geografic și la stradă; • afișarea stării de noduri sau un grup agregat de noduri; • vizualizarea topologiilor multicast folosind informații din lista dispozitivelor; • afișarea nu numai a stării dispozitivului pe hartă, ci și starea oricărui alt detaliu obținut prin interogarea de către utilizator a MIB.
Hardware acceptate	• controlul diferitor dispozitive de stocare: DELL, HP, IBM, NetApp, Pure Storage, Oracle și etc.; • detectarea aplicațiilor și controlul acestora utilizând șabloane de monitorizare încorporate bazate pe cele mai bune recomandări și experiență de operare; • dispozitivele detectate să identifice ca dispozitive ale unui producător specific și clasificate automat; • programul sistemului nu trebuie să provină de la o anumită companie furnizor; • software-ul sistemului nu trebuie să reflecte specificul unei anumite aplicații.
Extinderea funcționalității	• disponibilitatea API pentru importarea / exportarea nodurilor programate și pentru îndeplinirea funcțiilor similare; • regăsirea proprietăților de pe dispozitive fără a fi nevoie de importarea dispozitivelor MIB în baza de date MIB; • obținerea proprietăților de virtualizare și configurația acestora în tabloul de bord folosind capabilități avansate de căutare; • acordarea dreptului utilizatorilor de a personaliza valori, alerte și rapoarte pentru a extinde funcționalitatea standard; • obținerea valorilor în timp real sub formă de diagrame, precum și alerte pentru aceste proprietăți personalizate; • căutarea tuturor punctelor finale pe subrețele; • folosirea scripturilor personalizate pentru extensia de control a aplicației; • colectarea informațiilor despre clasificarea datelor de pe

	dispozitivele NAS care nu sunt acceptate în mod nativ; • colectarea proprietăților personalizate de pe dispozitive compatibile SNMP prin specificarea caracteristicilor OID-urilor.
Sisteme și servicii de monitorizare	• identificaree și clasificarea cel puțin 1200 de aplicații în mod implicit; • afișarea valorilor de volum agregate pentru fiecare aplicație / nod; • vizualizarea timpului de răspuns din rețea și timpului de răspuns ai programului pentru aplicațiile critice pentru misiune
Integrarea cu infrastructura	• integrarea cu software de monitorizare a aplicației pentru a oferi o vizualizare detaliată a performanței aplicației de la aplicație la mașină virtuală și la gazdă; • integrare cu ServiceNow etc. cu capacitatea de a crea automat incidente și sincronizarea bidirecțională a confirmării incidentului; • integrare cu alte module de monitorizare pentru a oferi o vedere detaliată a performanței aplicației de la stocare la gazdă, cu capacitatea de a suporta discuri MBR și GPT; • integrarea cu soluțiile de monitorizare a rețelei și a sistemelor pentru a crea un tablou de bord dinamic care oferă vizibilitate profundă și corelarea diferitelor puncte de date istorice în diferite părți ale infrastructurii; • integrarea cu module destinate altor componente, precum și furnizarea afișării dintr-o singură fereastră; • integrarea cu Active Directory / LDAP pentru autentificarea utilizatorului în programul de monitorizare; • integrarea cu software de monitorizare a platformei de virtualizare pentru a oferi o vizualizare granulară a performanței aplicației de la aplicație la mașină virtuală la gazdă; • integrarea cu aplicații terțe la nivel de interfață utilizând mesagerie și AIS; • integrarea cu aplicații de la alți producători: ServiceNow sau Matrix42; • automatizarea fluxului de lucru: o simplificarea gestionării adreselor IP ale mașinilor virtuale; o automatizarea alocării adreselor IP către o mașină virtuală; o automatizarea urmăririi înregistrărilor DNS ale mașinilor virtuale.
Scalabilitate	• furnizarea de performanță pentru stocarea pe termen lung și recuperarea mesajelor jurnal de ieșire; • extinderea rețelei prin adăugarea de suplimente / componente pentru echilibrarea sarcinii; • suport pentru mai multe opțiuni de implementare: o implementare centralizată; o implementare distribuită; o implementare hibridă. • disponibilitatea unei vizualizări centralizate a consolei de operare, o interfață pentru confirmarea alertelor și rapoartelor; • combinarea informațiilor din mai multe instanțe ale aplicației într-o singură vizualizare; • disponibilitatea mecanismelor de echilibrare a sarcinii și prelucrarea datelor fără a întrerupe comunicarea între server și aplicația principală; • monitorizarea mediilor distribuite la scară largă cu peste 10.000 de mașini virtuale; • monitorizare și scalabilitate de la medii mici (<100 utilizatori) la medii mari (40.000 utilizatori);

	• gestionarea a peste 15.000 de discuri; • Creșterea prin adăugarea de aplicații de echilibrare a sarcinii.
Valabilitate ridicată	• asigurarea disponibilității ridicate a aplicațiilor cu / fără utilizarea produselor de toleranță la erori.
Siguranță	• compatibilitate deplină cu TLS 1.2 fără nicio dependență de TLS 1.1 sau 1.0; • Asistență Microsoft Device Guard cu toate semnăturile binare pentru a asigura integritatea codului.
Implementarea platformei	• implementare în decurs de o oră fără ajutorul specialiștilor pentru implementare, implementare, personalizare sau personalizare; • Disponibilitate un tablou de bord activ care verifică automat platforma de monitorizare și afișează recomandări pentru corectarea articolelor neconforme; • Disponibilitate agent de completare pentru Windows, Linux (x86), Linux (ARM) și AIX; • a sustine implementare fără agent; • a sustine Implementări în Amazon EC2 și Microsoft Azure (opțional) • a sustine actualizare centralizată a tuturor componentelor la distanță, cum ar fi colector de date la distanță, consolă web fără gestionare suplimentară pe servere la distanță; • upgrade ușor și simplu la versiunile ulterioare.
Actualizări și asistență	• notificare în consolă web despre disponibilitatea noilor versiuni; • acordarea caracteristicilor noi cel puțin de două ori pe an sau mai mult; • acordarea și primirea consultărilor prin forumuri; • suport 24/7 printr-un portal de utilizator privat.
Gestionarea și auditarea drepturilor	• disponibilitatea funcțiilor pentru următoarele operațiuni: o automatizarea gestionării drepturilor de acces; o analiza și identificarea conturilor nesigure; o furnizarea înregistrărilor de audit pentru utilizatori, cu acces la date critice și confidențiale. • controlul, analiza și verificarea drepturilor de acces la Active Directory și la politica de grup Active Directory; • controlul, analiza și verificarea drepturilor de acces la partajarea fișierelor Windows; • controlul în timp real al tuturor acțiunilor de acces la resursele Active Directory, Windows, mape partajate; • urmărirea tuturor modificărilor efectuate în afara instrumentului de gestionare a permisiunilor utilizate, de exemplu, instrumentele Windows încorporate; • reprezentare grafică a relațiilor de permisiune a utilizatorilor și grupurilor din Active Directory, inclusiv grupuri suprapuse; • afișarea interactivă a relațiilor dintre resurse, structura acestora, conturi / grupuri de utilizatori și permisiuni; • suport pentru mai multe domenii Active Directory; • furnizarea recomandărilor și măsurilor pentru eliminarea amenințărilor de securitate identificate; • utilizarea portalului de gestionare web pentru delegarea operațiunilor standard de gestionare a conturilor, cum ar fi: resetarea parolei, solicitarea dreptului de acces la resurse, aprobarea cererii dreptului de acces; • gestionare ușoară în configurarea rolurilor, ștergerea conturilor și

	permisiunilor utilizatorilor; • verificarea periodică a drepturilor de acces ale tuturor angajaților la resurse; • disponibilitatea funcției de a trimite comentarii pentru toate modificările manuale pentru confirmare documentară; • afișare în timp real a notificărilor despre accesuri autorizate și neconfirmate sau modificări ale resurselor: Active Directory, Exchange și Windows, foldere partajate; • identificarea utilizării greșite a acreditării și a altor acțiuni neautorizate / suspecte; • detectarea și raportarea potențialelor riscuri la acreditări, de exemplu, pentru conturile cu configurații nesigure; • asistență pentru trimiterea e-mailurilor, intrări de jurnal de evenimente Windows și scripturi la generarea de alerte.