Anexa nr. 22
la Documentația standard
aprobată prin Ordinul Ministrului Finanțelor
nr. 115 din 15.09.2021

**Specificații tehnice**

**Numărul procedurii de achiziție:** ***ocds-b3wdp1-MD-1784732374102 (21658469) din 22.07.2026***

**Obiectul achiziției:** ***Pachete software antivirus***

| Denumirea bunurilor/ serviciilor | Denumirea bunurilor/ serviciilor | Țara de origine | Producă-torul | Specificarea tehnică deplină solicitată de către autoritatea contractantă | Specificarea tehnică deplină propusă de către ofertant | Standarde de referință |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **Lotul nr. 1 - Pachete software antivirus** | | | | | | |
| **Pachete software antivirus (inclusiv Disk Encryption management)** | ESET PROTECT Enterprise | Slovakia | ESET | Conform caietului de sarcini și clarificarilor la Anunțul de participare<br><br>**<u>Tip</u>:** Subscriere anuală pentru soluția de protecție și securitate pentru 1000 entități (PC/ laptop/ VDI/ Server) pentru perioada de 3 ani.<br>**<u>Cantitate:</u>** Ofertantului este responsabil de a determinarea modelului de licențiere luând în calcul:<br>• 1000 entități *(PC/laptop/VDI/Server);*<br>• Disk Encryption management pentru 1000 entități. | **ESET PROTECT Enterprise On-premise 1000 obj/ 3 years**<br><br>**<u>Tip</u>:** Subscriere anuală pentru soluția de protecție și securitate pentru 1000 entități (PC/ laptop/ VDI/ Server) pentru perioada de 3 ani.<br>**<u>Cantitate:</u>** Modelul de licențiere:<br>• 1000 entități *(PC/laptop/VDI/Server);*<br>• Disk Encryption management pentru 1000 entități.<br><br>Produsul antivirus ESET ocupa locurile de top în testele internaționale independente cu | N/A |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaţionale independente cu renume mondial în domeniu *(certificări "AV-TEST", "VIRUS BULLETIN'S", "REAL-WORLD PROTECTION", "MALWARE PROTECTION").*<br><br>***<u>Caracteristici generale ale produsului:</u>***<br><br>Soluţia trebuie să reprezinte o platformă integrată pentru managementul securităţii, gândită ca o soluţie modulară.<br>Produsul va conţine următoarele module, toate cu posibilitatea de a fi gestionate şi administrate dintr-o singură consolă de management:<br>• Protecţie staţii şi servere fizice şi virtualizate;<br>• Serviciu de corelare şi răspuns la evenimente de tip EDR *(endpoint detection and response).*<br>*[Raspuns clarificare (5 aug 2026, 10:20) Consola de management trebuie să asigure administrarea,* | renume mondial în domeniu *(certificări "AV-TEST", "VIRUS BULLETIN'S", "REAL-WORLD PROTECTION", "MALWARE PROTECTION").*<br><br>***<u>Caracteristici generale ale produsului:</u>***<br><br>Soluţia reprezinta o platformă integrată pentru managementul securităţii, gândită ca o soluţie modulară.<br>Produsul conţine următoarele module, toate cu posibilitatea de a fi gestionate şi administrate dintr-o singură consolă de management:<br>• Protecţie staţii şi servere fizice şi virtualizate;<br>• Serviciu de corelare şi răspuns la evenimente de tip EDR *(endpoint detection and response).*<br>*[Raspuns clarificare (5 aug 2026, 10:20) Consola de management asigura administrarea, monitorizarea şi gestionarea centralizată a tuturor modulelor şi componentelor soluţiei propuse.* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | *monitorizarea și gestionarea centralizată a tuturor modulelor și componentelor soluției propuse. Totodată, pentru funcționalitățile specializate ale anumitor module, este permisă redirecționarea administratorului către console dedicate, cu condiția menținerii unui sistem unificat de administrare și control.]*<br><br>***<u>Consola de management:</u>***<br><br>Accesibilitate atât de pe browser desktop cât și tip mobile.<br>Să ofere opțiune configurabilă de actualizare automată a consolei de management.<br><br>***<u>Soluția de scanare centralizată:</u>***<br><br>Soluția trebuie să asigure protecția mediilor virtualizate *(VDI)*, inclusiv a mediilor persistente și non-persistente, și să fie compatibilă cu următoarele platforme de virtualizare:<br>**1.** VMware vSphere;<br>**2.** Citrix XenServer; | *Totodată, pentru funcționalitățile specializate ale anumitor module, este permisă redirecționarea administratorului către console dedicate, cu condiția menținerii unui sistem unificat de administrare și control.]*<br><br>***<u>Consola de management:</u>***<br><br>Accesibilitate atât de pe browser desktop cât și tip mobile.<br>Ofera opțiunea configurabilă de actualizare automată a consolei de management.<br><br>***<u>Soluția de scanare centralizată:</u>***<br><br>Soluția asigura protecția mediilor virtualizate *(VDI)*, inclusiv a mediilor persistente și non-persistente, și este compatibilă cu următoarele platforme de virtualizare:<br>**1.** VMware vSphere;<br>**2.** Citrix XenServer;<br>**3.** Microsoft Hyper-V. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **3.** Microsoft Hyper-V.<br>*[Raspuns Clarificare (5 aug 2026, 10:19): Având în vedere evoluția soluțiilor moderne de securitate, Autoritatea Contractantă acceptă atât protecția bazată pe integrarea directă cu platforma de virtualizare, cât și protecția realizată prin intermediul unui agent instalat și administrat centralizat în sistemul de operare invitat. Cerința va fi considerată îndeplinită dacă soluția oferă protecție completă și administrare centralizată, indiferent de tehnologia de virtualizare utilizată.]*<br>*[Raspuns Clarificare (5 aug 2026, 10:23): Cerința va fi considerată îndeplinită dacă soluția asigură protecția completă și administrarea centralizată a mașinilor virtuale, indiferent de platforma de virtualizare utilizată sau de mecanismul de protecție implementat. Suportul parțial sau suportul pentru o singură platformă va fi considerat conform cerințelor tehnice.]* | *[Raspuns Clarificare (5 aug 2026, 10:19): Având în vedere evoluția soluțiilor moderne de securitate, Autoritatea Contractantă acceptă atât protecția bazată pe integrarea directă cu platforma de virtualizare, cât și protecția realizată prin intermediul unui agent instalat și administrat centralizat în sistemul de operare invitat. Cerința va fi considerată îndeplinită dacă soluția oferă protecție completă și administrare centralizată, indiferent de tehnologia de virtualizare utilizată.]*<br>*[Raspuns Clarificare (5 aug 2026, 10:23): Cerința va fi considerată îndeplinită dacă soluția asigură protecția completă și administrarea centralizată a mașinilor virtuale, indiferent de platforma de virtualizare utilizată sau de mecanismul de protecție implementat. Suportul parțial sau suportul pentru o singură platformă va fi considerat conform cerințelor tehnice.]* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | ***Cerinţe generale produs:***<br>Soluţia trebuie să:<br>• permită activarea/dezactivarea actualizărilor automate de produs/semnături şi a consolei de management;<br>• ofere vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcţii noi si îmbunătăţiri, probleme rezolvate, probleme cunoscute;<br>• afişeze notificările şi alertele existente, să alerteze administratorul în cazul unor probleme majore *(configurabile)*: licenţiere, detecţie viruşi, actualizări de produs disponibile.<br>***Panou de monitorizare si raportare (Dashboard):***<br>• să ofere posibilitatea creării rapoartelor configurabile după tip, ţintă şi scop cu opţiuni specifice pentru orice tip de raport cu posibilităţi de | ***Cerinţe generale produs:***<br>Soluţia propusa:<br>• Permite activarea/dezactivarea actualizărilor automate de produs/semnături şi a consolei de management;<br>• ofera vizualizarea unui jurnal de modificări în care sunt precizate istoric: versiunea consolei de management, data versiunii, funcţii noi si îmbunătăţiri, probleme rezolvate, probleme cunoscute;<br>• afişeaza notificările şi alertele existente, alerteaza administratorul în cazul unor probleme majore *(configurabile)*: licenţiere, detecţie viruşi, actualizări de produs disponibile.<br>***Panou de monitorizare si raportare (Dashboard):***<br>• ofera posibilitatea creării rapoartelor configurabile după tip, ţintă şi | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | adăugare/eliminare şi rearanjare.<br>• să prezinte rapoarte pentru toate modulele suportate *(stare/statut/actualizare)*.<br>***<u>Inventarierea reţelei – managementul securităţii:</u>***<br>Produsul trebuie să:<br>• se integreze cu domenii Active Directory multiple, să poată importa inventarul.<br>• permită descoperirea PC neintegrate în Active Directory (Workgroup);<br>• ofere opţiuni de căutare, sortare şi filtrare după numele sistemului, sistem de operare si adresa IP, politica aplicată, online şi/sau offline şi FQDN;<br>• permită instalarea la distanţă sau manual a clienţilor antivirus pe maşini fizice şi virtuale;<br>• permită selectarea modulelor componente atunci când se creează pachetul clientului care se instalează pe maşinile fizice/virtuale; | scop cu opţiuni specifice pentru orice tip de raport cu posibilităţi de adăugare/eliminare şi rearanjare.<br>• prezinta rapoarte pentru toate modulele suportate *(stare/statut/actualizare)*.<br>***<u>Inventarierea reţelei – managementul securităţii:</u>***<br>Produsul poate să:<br>• integreze cu domenii Active Directory multiple, poate importa inventarul.<br>• permite descoperirea PC neintegrate în Active Directory (Workgroup);<br>• ofera opţiuni de căutare, sortare şi filtrare după numele sistemului, sistem de operare si adresa IP, politica aplicată, online şi/sau offline şi FQDN;<br>• permite instalarea la distanţă sau manual a clienţilor antivirus pe maşini fizice şi virtuale;<br>• permite selectarea modulelor componente atunci când se creează pachetul | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • permită lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanţă pentru clientul antivirus;<br>• ofere posibilitatea de repornire a maşinilor fizice de la distanţă;<br>• ofere informaţii detaliate despre fiecare task iniţiat şi afişarea statutului lui;<br>• permită configurarea centralizată a clienţilor antivirus prin intermediul politicilor;<br>• ofere în consola de management informaţii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături;<br>• permită descoperirea tuturor aplicaţiilor instalate pe toate staţiile şi serverele din reţea.<br><br>***<u>Politici:</u>***<br><br>Produsul trebuie să:<br>• permită configurarea setărilor clientului antivirus prin | clientului care se instalează pe maşinile fizice/virtuale;<br>• permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalare la distanţă pentru clientul antivirus;<br>• ofera posibilitatea de repornire a maşinilor fizice de la distanţă;<br>• ofera informaţii detaliate despre fiecare task iniţiat şi afişarea statutului lui;<br>• permite configurarea centralizată a clienţilor antivirus prin intermediul politicilor;<br>• ofera în consola de management informaţii detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături;<br>• permite descoperirea tuturor aplicaţiilor instalate pe toate staţiile şi serverele din reţea. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | intermediul unei singure politici ce conţine setări pentru toate module;<br>• conţină opţiuni specifice de activare/dezactivare şi configurare a funcţionalităţilor precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicaţiilor, scanarea traficului web, controlul dispozitivelor, power user;<br>• permită aplicarea politicilor pe maşini client, grupuri de maşini, pool-uri de resurse (VMware), domeniu, unităţi organizaţionale sau useri de active directoy;<br>*[Raspuns clarificare (5 aug 2026, 10:19) Cerința referitoare la aplicarea politicilor asupra pool-urilor de resurse VMware a fost stabilită pentru a asigura flexibilitatea administrării infrastructurii IT. Totodată, Autoritatea Contractantă constată că acelaşi rezultat funcţional poate fi obţinut prin utilizarea grupurilor de dispozitive, grupurilor dinamice,* | ***Politici:***<br>Produsul poate să:<br>• permită configurarea setărilor clientului antivirus prin intermediul unei singure politici ce conţine setări pentru toate module;<br>• conţine opţiuni specifice de activare/dezactivare şi configurare a funcţionalităţilor precum scanarea antivirus la cerere, firewall, controlul accesului la Internet, controlul aplicaţiilor, scanarea traficului web, controlul dispozitivelor, power user;<br>• permite aplicarea politicilor pe maşini client, grupuri de maşini, pool-uri de resurse (VMware), domeniu, unităţi organizaţionale sau useri de active directoy;<br>*[Raspuns clarificare (5 aug 2026, 10:19) Cerința referitoare la aplicarea politicilor asupra pool-urilor de resurse VMware a fost stabilită pentru a asigura flexibilitatea administrării infrastructurii IT. Totodată,* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | *etichetelor, domeniilor sau unităţilor organizaţionale Active Directory. În consecinţă, vor fi acceptate şi mecanisme echivalente de grupare şi administrare a politicilor, cu condiţia asigurării unui nivel similar de funcţionalitate.]*<br>• poată fi schimbată automat în funcţie de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în accesai reţea cu infrastructura de management, Tipul reţelei (lan, wireless).<br>***<u>Monitorizare şi raportare:</u>***<br>Produsul trebuie să:<br>• permită setarea de opţiuni specifice pentru afişarea rapoartelor existente;<br>• deţină un panou central care să afişeze statutul modulelor şi rapoartele lor pentru perioadele de timp specificate;<br>• conţină rapoarte care prezinta statutul maşinilor clienţilor, al actualizărilor, fişierelor malware detectate, | *Autoritatea Contractantă constată că acelaşi rezultat funcţional poate fi obţinut prin utilizarea grupurilor de dispozitive, grupurilor dinamice, etichetelor, domeniilor sau unităţilor organizaţionale Active Directory. În consecinţă, vor fi acceptate şi mecanisme echivalente de grupare şi administrare a politicilor, cu condiţia asigurării unui nivel similar de funcţionalitate.]*<br>• poate fi schimbată automat în funcţie de: User-ul logat, IP sau clasa de IP, Gateway-ul alocat, DNS serverul alocat, Clientul este/nu este în accesai reţea cu infrastructura de management, Tipul reţelei (lan, wireless).<br>***<u>Monitorizare şi raportare:</u>***<br>Produsul ofertat:<br>• permite setarea de opţiuni specifice pentru afişarea rapoartelor existente;<br>• deţine un panou central care să afişeze statutul modulelor şi rapoartele lor | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | aplicaţiile blocate, site-urilor web blocate;<br>• trimită rapoarte către un număr nelimitat de adrese de email;<br>• permită vizualizarea rapoartelor curente programate de administrator;<br>• permită exportarea rapoartelor în format .pdf si detaliile ca format .csv;<br>• includă un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menţinând informaţiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal;<br>• ofere interogări legate de starea terminalului precum: tip maşină, infrastructură reţelei căreia aparţine, datele agentului de securitate, starea modulelor de protecţie, rolurile terminalelor;<br>• ofere interogări legate de evenimente precum: calculatorul | pentru perioadele de timp specificate;<br>• conţine rapoarte care prezinta statutul maşinilor clienţilor, al actualizărilor, fişierelor malware detectate, aplicaţiile blocate, site-urilor web blocate;<br>• trimite rapoarte către un număr nelimitat de adrese de email;<br>• permite vizualizarea rapoartelor curente programate de administrator;<br>• permite exportarea rapoartelor în format .pdf si detaliile ca format .csv;<br>• include un generator de rapoarte care să ofere posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menţinând informaţiile concise si ordonate corespunzător, să includă interogări precum: starea terminalului, evenimente terminal;<br>• ofera interogări legate de starea terminalului precum: tip maşină, infrastructură | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | ţinta pe care a avut loc evenimentul, tipul starea şi configuraţia agentului de securitate instalat, starea modulelor şi rolurilor de protecţie instalate pe agentul de securitate, denumirea şi alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicaţii blocate, detecţiile etc);<br><br>***<u>Carantină:</u>***<br><br>• Produsul trebuie să permită restaurarea fişierelor din carantină în locaţia originală sau într-o cale configurabilă;<br>• Administrarea Carantinei să fie posibilă atât pe terminalul administrat cât şi din consola de management;<br><br>***<u>Utilizatori:</u>***<br><br>• Administrarea este necesar să fie efectuată pe bază de roluri multiple predefinite: Administrator companie, Administrator reţea, Reporter şi alte roluri configurabile detaliat cu posibilitatea de selectare a | reţelei căreia aparţine, datele agentului de securitate, starea modulelor de protecţie, rolurile terminalelor;<br>• ofera interogări legate de evenimente precum: calculatorul ţinta pe care a avut loc evenimentul, tipul starea şi configuraţia agentului de securitate instalat, starea modulelor şi rolurilor de protecţie instalate pe agentul de securitate, denumirea şi alocarea politicii, utilizatorul autentificat în timpul evenimentului, evenimente (site-uri blocate, aplicaţii blocate, detecţiile etc);<br><br>***<u>Carantină:</u>***<br><br>• Produsul permite restaurarea fişierelor din carantină în locaţia originală sau într-o cale configurabilă;<br>• Administrarea Carantinei este posibilă atât pe terminalul administrat cât şi din consola de management;<br><br>***<u>Utilizatori:</u>*** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | serviciilor și obiectelor pentru care un utilizator poate face modificări;<br>• Utilizatorii să poată fi importaţi din Microsoft Active Directory sau creaţi în consola de management;<br>• Să fie posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp - configurabil.<br>*[Raspuns clarificare (5 aug 2026, 10:22): Prin „deconectare automată" se înțelege închiderea automată a sesiunii utilizatorului din consola de management după expirarea unei perioade configurabile de inactivitate sau după expirarea intervalului de timp stabilit.]*<br>*[Raspuns clarificare (5 aug 2026, 10:23): Prin „deconectare automată" se înțelege închiderea automată a sesiunii utilizatorului din consola de management după expirarea unei perioade configurabile de inactivitate sau după expirarea intervalului de timp stabilit.]* | • Administrarea poate să fie efectuată pe bază de roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter și alte roluri configurabile detaliat cu posibilitatea de selectare a serviciilor și obiectelor pentru care un utilizator poate face modificări;<br>• Utilizatorii pot fi importaţi din Microsoft Active Directory sau creaţi în consola de management;<br>• Este posibilă deconectarea automată a oricărui tip de utilizator după un anumit timp - configurabil.<br>*[Raspuns clarificare (5 aug 2026, 10:22): Prin „deconectare automată" se înțelege închiderea automată a sesiunii utilizatorului din consola de management după expirarea unei perioade configurabile de inactivitate sau după expirarea intervalului de timp stabilit.]*<br>*[Raspuns clarificare (5 aug 2026, 10:23): Prin „deconectare automată" se înțelege închiderea* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **<u>Log-uri:</u>**<br>• Soluția trebuie să permită înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare.<br>*[Raspuns clarificare (5 aug 2026, 10:22): Soluția trebuie să asigure înregistrarea acțiunilor utilizatorilor în consola de management, inclusiv autentificarea și deconectarea, crearea, modificarea și ștergerea obiectelor, modificarea politicilor și setărilor, executarea operațiunilor administrative, precum și informații privind utilizatorul, data și ora efectuării acțiunii și rezultatul acesteia. Jurnalul trebuie să fie disponibil pentru vizualizare și export.]*<br>*[Raspuns clarificare (5 aug 2026, 10:24): Soluția trebuie să asigure înregistrarea acțiunilor utilizatorilor în consola de management, inclusiv autentificarea și deconectarea, crearea, modificarea și ștergerea* | *automată a sesiunii utilizatorului din consola de management după expirarea unei perioade configurabile de inactivitate sau după expirarea intervalului de timp stabilit.]*<br>**<u>Log-uri:</u>**<br>• Soluția permite înregistrarea acțiunilor utilizatorilor și să ofere informații detaliate pentru fiecare acțiune a unui utilizator cu posibilitatea de filtrare.<br>*[Raspuns clarificare (5 aug 2026, 10:22): Soluția trebuie să asigure înregistrarea acțiunilor utilizatorilor în consola de management, inclusiv autentificarea și deconectarea, crearea, modificarea și ștergerea obiectelor, modificarea politicilor și setărilor, executarea operațiunilor administrative, precum și informații privind utilizatorul, data și ora efectuării acțiunii și rezultatul acesteia. Jurnalul trebuie să fie disponibil pentru vizualizare și export.]* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | *obiectelor, modificarea politicilor şi setărilor, executarea operaţiunilor administrative, precum şi informaţii privind utilizatorul, data şi ora efectuării acţiunii şi rezultatul acesteia. Jurnalul trebuie să fie disponibil pentru vizualizare şi export.]*<br><br>***<u>Actualizare:</u>***<br>Soluţia va permite:<br>• Definirea de locaţii de actualizare multiple;<br>• Activarea/dezactivarea actualizărilor;<br>• Testarea noilor versiuni înainte de a fi instalate pe toţi clienţii *(posibilitate de actualizare în mai multe cicluri – 1 mediu de test, 2 – mediu de producţie);*<br>• Definirea zonelor de test şi zonelor critice de producţie.<br>***<u>Protecţie staţii şi servere fizice si virtualizate – caracteristici minime:</u>***<br>Soluţia trebuie să: | *[Raspuns clarificare (5 aug 2026, 10:24): Soluţia trebuie să asigure înregistrarea acţiunilor utilizatorilor în consola de management, inclusiv autentificarea şi deconectarea, crearea, modificarea şi ştergerea obiectelor, modificarea politicilor şi setărilor, executarea operaţiunilor administrative, precum şi informaţii privind utilizatorul, data şi ora efectuării acţiunii şi rezultatul acesteia. Jurnalul trebuie să fie disponibil pentru vizualizare şi export.]*<br><br>***<u>Actualizare:</u>***<br>Soluţia permite:<br>• Definirea de locaţii de actualizare multiple;<br>• Activarea/dezactivarea actualizărilor;<br>• Testarea noilor versiuni înainte de a fi instalate pe toţi clienţii *(posibilitate de actualizare în mai multe cicluri –* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Permită instalarea personalizată a modulelor;<br>• Includă un „vaccin” anti-ransomware, cu actualizări de la producător, pentru protecţia împotriva tuturor ameninţărilor cunoscute de tip ransomware, prin imunizarea staţiilor şi serverelor, chiar daca sunt infectate şi blocarea procesului de criptare;<br>• Includă protecţie împotriva atacurilor zero-day de tip exploit *(atacuri direcţionate);*<br>• Includă modul de analiză la risc capabil să identifice şi să remedieze riscurile identificate la nivel de reţea sau sistem de operare, cu posibilitate de configurare şi automatizare;<br>• Includă un modul avansat de securitate bazat pe tehnologii de machine learning, analiză comportamentală şi algoritmi euristici, proiectat pentru detectarea atacurilor avansate şi a activităţilor suspecte înainte de faza de execuţie;<br>• Includă modul avansat de securitate pentru protecţie | *1 mediu de test, 2 – mediu de producţie);*<br>• Definirea zonelor de test şi zonelor critice de producţie.<br>***<u>Protecţie staţii şi servere fizice si virtualizate – caracteristici minime:</u>***<br>Soluţia:<br>• Permite instalarea personalizată a modulelor;<br>• Include un „vaccin” anti-ransomware, cu actualizări de la producător, pentru protecţia împotriva tuturor ameninţărilor cunoscute de tip ransomware, prin imunizarea staţiilor şi serverelor, chiar daca sunt infectate şi blocarea procesului de criptare;<br>• Include protecţie împotriva atacurilor zero-day de tip exploit *(atacuri direcţionate);*<br>• Include modul de analiză la risc capabil să identifice şi să remedieze riscurile identificate la nivel de reţea sau sistem de operare, cu | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | împotriva: atacurilor direcţionate *(Targeted Attack),* fişierelor suspecte si traficului la nivel de reţea suspect, exploit-urilor, ransomware şi grayware. Fiecărui tip de ameninţare trebuie să i se poată configura independent nivelul de protecţie şi acţiunile aplicate, în funcţie de capabilităţile soluţiei ofertate şi recomandările producătorului;<br>• Includă modul de sandbox, unde se vor putea trimite manual sau automat fişiere pentru a putea fi „detonate" pentru o analiză în profunzime;<br>*[Raspuns clarificare (5 aug 2026, 10:23) Soluţia trebuie să fie implementată în infrastructura (on-premises).]*<br>*[Raspuns clarificare (5 aug 2026, 10:24): Da, soluţia trebuie să permită atât transmiterea manuală, cât şi transmiterea automată a fişierelor către modulul Sandbox, pentru a asigura analiza completă a obiectelor suspecte.]* | posibilitate de configurare şi automatizare;<br>• Include un modul avansat de securitate bazat pe tehnologii de machine learning, analiză comportamentală şi algoritmi euristici, proiectat pentru detectarea atacurilor avansate şi a activităţilor suspecte înainte de faza de execuţie;<br>• Include modul avansat de securitate pentru protecţie împotriva: atacurilor direcţionate *(Targeted Attack),* fişierelor suspecte si traficului la nivel de reţea suspect, exploit-urilor, ransomware şi grayware. Fiecărui tip de ameninţare i se poate configura independent nivelul de protecţie şi acţiunile aplicate, în funcţie de capabilităţile soluţiei ofertate şi recomandările producătorului;<br>• Include modul de sandbox, unde se vor putea trimite manual sau automat fişiere pentru a putea fi | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Includă variante de analiză a sandbox-ului tip: doar monitorizare sau blocare cu acţiuni de remediere: implicită şi de siguranţa. Pentru acţiunea implicită: doar raportare, dezinfecţie, ştergere şi transmitere în carantină. Pentru acţiunea de siguranţa: ştergere sau permutare în carantină;<br>• Suporte ”detonarea” în modulul sandbox, minim, tipurile de fişiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML *(Unicode),* JAR *(archive),* JS, LNK, MHTML *(doc),* MHTML *(ppt),* MHTML *(xls),* Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files *(executable),* PDF, PEF *(executable),* PIF *(executable),* RTF, SCR, URL *(binary),* VBE, VBS, WSF, WSH, WSH-VBS, XHTML. Acestea vor fi detectate corect chiar dacă vor fi în arhive de tipul : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, | „detonate” pentru o analiză în profunzime;<br>*[Raspuns clarificare (5 aug 2026, 10:23) Soluția trebuie să fie implementată în infrastructura (on-premises).]*<br>*[Raspuns clarificare (5 aug 2026, 10:24): Da, soluția trebuie să permită atât transmiterea manuală, cât şi transmiterea automată a fişierelor către modulul Sandbox, pentru a asigura analiza completă a obiectelor suspecte.]*<br>• Include variante de analiză a sandbox-ului tip: doar monitorizare sau blocare cu acţiuni de remediere: implicită şi de siguranţa. Pentru acţiunea implicită: doar raportare, dezinfecţie, ştergere şi transmitere în carantină. Pentru acţiunea de siguranţa: ştergere sau permutare în carantină;<br>• Suporta ”detonarea” în modulul sandbox, minim, tipurile de fişiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML *(Unicode),* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | Unix Z, ZIP, ZIP *(multivolume),* ZOO, XZ ;<br>• Ofere posibilitate de filtrare a incidentelor din interfaţa grafică în funcţie intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac, sistem de operare afectat cît şi după IP, nume fişier, nume staţie;<br>• Permită vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: să generează o hartă de principiu a incidentului, să detalieze incidentul în funcţie de amprenta de timp a fiecărei acţiuni aferente incidentului, să poată genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigare – virus total, sandbox, google – la nivel de fişier, adăugare în lista de blocare – la nivel de reţea sau instalare patch – la nivel de nod);<br>• Poată bloca fişiere şi/sau procese folosind valori hash de tip MD5/SHA256 direct din | JAR *(archive),* JS, LNK, MHTML *(doc),* MHTML *(ppt),* MHTML *(xls),* Microsoft Excel, Microsoft PowerPoint, Microsoft Word, MZ/PE files *(executable),* PDF, PEF *(executable),* PIF *(executable),* RTF, SCR, URL *(binary),* VBE, VBS, WSF, WSH, WSH-VBS, XHTML. Acestea vor fi detectate corect chiar dacă vor fi în arhive de tipul : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP *(multivolume),* ZOO, XZ ;<br>• Ofera posibilitatea de filtrare a incidentelor din interfaţa grafică în funcţie intervalul de timp, pe baza unui scor de încredere, indicatori de atac, tehnici de atac, sistem de operare afectat cît şi după IP, nume fişier, nume staţie;<br>• Permite vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod: să generează o hartă de principiu a | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | pagina aferentă incidentului sau importate folosind un fișier CSV;<br>• Poată excepta fișiere non-maliţioase de la acţiunea de investigare sau poate genera/adaugă un set de fișiere maliţioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor maliţioase;<br>• Permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru a permite o investigare rapidă a gazdei/ colectare date despre atacul respectiv/ remediere în timp real a breșelor de securitate/ permită executarea unor comenzi în linia de comandă care se execută cu privilegii de kernel pentru eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare;<br>• Permită crearea regulilor de detecţie customizabilă bazată pe procese, fișiere, registre și conexiuni de rețea; | incidentului, să detalieze incidentul în funcţie de amprenta de timp a fiecărei acțiuni aferente incidentului, să poată genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigare – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod);<br>• Poate bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;<br>• Poate excepta fișiere non-maliţioase de la acţiunea de investigare sau poate genera/adaugă un set de fișiere maliţioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor maliţioase;<br>• Permite deschiderea unei conexiuni remote către un | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Permită creare regulilor de excludere customizabilă bazată pe procese, fișiere, registre si conexiuni de rețea;<br>• Permită căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre;<br>• Permită deschiderea unei conexiuni remote către un endpoint potențial infectat pentru investigare rapidă, colectare date și remedierea în timp real a breșei de securitate, reducând timpul de remediere (downtime) în cazul unui atac, executarea comenzilor în linia de comandă cu privilegii de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare;<br>• Includă modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response”) capabil să identifice | endpoint potențial infectat pentru a permite o investigare rapidă a gazdei/ colectare date despre atacul respectiv/ remediere în timp real a breșelor de securitate/ permită executarea unor comenzi în linia de comandă care se execută cu privilegii de kernel pentru eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare;<br>• Permite crearea regulilor de detecție customizabilă bazată pe procese, fișiere, registre și conexiuni de rețea;<br>• Permite creare regulilor de excludere customizabilă bazată pe procese, fișiere, registre si conexiuni de rețea;<br>• Permite căutarea pro activă pe endpoint-urile protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registre, valori de registre; | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | ameninţări avansate sau atacuri în curs de desfăşurare. Acest modul va fi capabil să:<br>***a)*** *cuprindă colectarea de date şi evenimente despre hardware şi software aferent fiecărei staţii de lucru aducând informaţii detaliate referitoare la incidentele detectate, o hartă detaliata a acestora precum şi acţiuni de remediere automate şi integrare cu modulele de Sandbox şi modulul avansat de securitate;*<br>***b)*** *ofere senzori de colectare a datelor şi componente de procesare şi interpretare a acestora;*<br>***c)*** *posede capacitarăţi de evaluare a activităţii tipice a unui endpoint din perspectiva securităţii acestuia conform tehnicilor de atac MITRE („baselining”) şi va raporta orice deviaţie de la acest comportament sub forma unui incident;* | • Permite deschiderea unei conexiuni remote către un endpoint potenţial infectat pentru investigare rapidă, colectare date şi remedierea în timp real a breşei de securitate, reducând timpul de remediere (downtime) în cazul unui atac, executarea comenzilor în linia de comandă cu privilegii de kernel ce permit eliminarea în timp real a unor ameninţări sau colectarea de date privitoare la atacul în desfăşurare;<br>• Include modul de detectare, corelare şi răspuns la evenimente de tip EDR („endpoint detection and response”) capabil să identifice ameninţări avansate sau atacuri în curs de desfăşurare. Acest modul este capabil să:<br>***h)*** *cuprindă colectarea de date şi evenimente despre hardware şi software aferent fiecărei staţii de lucru aducând informaţii detaliate referitoare la incidentele detectate, o hartă detaliata a acestora* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | ***d)*** *ofere vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat generînd o hartă de principiu a incidentului, detaliind incidentul în funcție de amprenta de timp a fiecărei actiuni aferente incidentului, respectiv butonul „acționează" care poate genera un set de masuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod);*<br>***e)*** *poate bloca fișiere si/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV;*<br>***f)*** *poată excepta fișiere non-malițioase de la* | *precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate;*<br>***i)*** *ofera senzori de colectare a datelor și componente de procesare și interpretare a acestora;*<br>***j)*** *poseda capacitarăți de evaluare a activității tipice a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și va raporta orice deviație de la acest comportament sub forma unui incident;*<br>***k)*** *ofera vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat generînd o hartă de principiu a incidentului, detaliind incidentul în funcție de amprenta de timp a fiecărei actiuni aferente incidentului, respectiv butonul* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | *acţiunea de investigare sau poate genera/adaugă un set de fişiere maliţioase într-o listă pentru a preveni mişcarea laterală a fişierelor/proceselor maliţioase;*<br>***g)*** *permită vizualizarea incidentelor extinse corelate de pe mai multe endpoint-uri.*<br><br>***<u>Cerinţe de sistem:</u>***<br><br>• Sisteme de operare pentru staţii de lucru: Windows 7/10/11 (inclusiv Embebed şi IoT), Mac OS X de la 10.12 şi mai recent, Red Hat Enterprise Linux / CentOS 7 şi mai recent, Oracle Linux 6.3 şi mai recent, Ubuntu 16 şi mai recent, SUSE Linux Enterprise Server 12 şi mai recent, OpenSUSE 15 şi mai recent, Fedora 31 şi mai recent;<br>• Sisteme de operare Windows pentru servere: Windows Server 2012/2012 R2/2016/2019/2022.<br>*[Raspuns clarificare (6 aug 2026, 10:52): Este obligatorie* | *„acţionează" care poate genera un set de masuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigaţi – virus total, sandbox, google – la nivel de fişier, adăugare în lista de blocare – la nivel de reţea sau instalare patch – la nivel de nod);*<br>***l)*** *poate bloca fişiere si/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fişier CSV;*<br>***m)*** *poate excepta fişiere non-maliţioase de la acţiunea de investigare sau poate genera/adaugă un set de fişiere maliţioase într-o listă pentru a preveni mişcarea laterală a fişierelor/proceselor maliţioase;*<br>***n)*** *permite vizualizarea incidentelor extinse* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | *asigurarea compatibilității cu sistemele de operare aflate în perioada de suport activ din partea producătorilor acestora. Suportul pentru arhitectura ARM nu reprezintă o cerință obligatorie. Compatibilitatea cu sistemele de operare pentru care producătorul a încetat oficial suportul (End-of-Life) este acceptată, însă nu constituie o cerință obligatorie.]*<br><br>***<u>Administrare și instalare remote:</u>***<br><br>• Pachetele de instalare trebuie să fie configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay” *(update server”);*<br>• Să existe posibilitatea de instalare manuală, sau automată la distanță, direct din consola de management;<br>• Din consola să fie disponibile informații despre fiecare endpoint: numele, IP, sistem de operare, module | *corelate de pe mai multe endpoint-uri.*<br><br>***<u>Cerințe de sistem:</u>***<br><br>• Sisteme de operare pentru stații de lucru: Windows 7/10/11 (inclusiv Embebed și IoT), Mac OS X de la 10.12 și mai recent, Red Hat Enterprise Linux / CentOS 7 și mai recent, Oracle Linux 6.3 și mai recent, Ubuntu 16 și mai recent, SUSE Linux Enterprise Server 12 și mai recent, OpenSUSE 15 și mai recent, Fedora 31 și mai recent;<br>• Sisteme de operare Windows pentru servere: Windows Server 2012/2012 R2/2016/2019/2022.<br>*[Raspuns clarificare (6 aug 2026, 10:52): Este obligatorie asigurarea compatibilității cu sistemele de operare aflate în perioada de suport activ din partea producătorilor acestora. Suportul pentru arhitectura ARM nu reprezintă o cerință obligatorie. Compatibilitatea cu sistemele de operare pentru care producătorul a încetat* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | instalate, politica aplicată, informaţii despre actualizări;<br>• Posibilităţi de creare kit pentru endpoint – tip: universar – 32/64bit, fizic/VDI, web installe/full;<br>• Gestionare, creare şi configurare grupuri pentru endpoint ce nu sunt în AD;<br>• Posibilitate de atribuire a funcţionalităţii de descoperire a endpointurilor şi în afara AD, pentru oricare endpoint.<br>***<u>Caracteristici şi funcţionalităţi principale ale modulului antivirus:</u>***<br>Produsul trebuie sa permită:<br>• Stabilirea acţiunilor întreprinse de modulul antivirus la detectarea unei ameninţări noi. Astfel administratorul va putea alege între următoarele acţiuni:<br>***a)*** *implicită pentru fişiere infectate: interzice accesul, dezinfectează, ştergere, mută fişierele în carantină, nici o acţiune;* | *oficial suportul (End-of-Life) este acceptată, însă nu constituie o cerinţă obligatorie.]*<br>***<u>Administrare şi instalare remote:</u>***<br>• Pachetele de instalare sunt configurabile cu modulele necesare cu domenii tip firewall, device control, power user, content control, disk encryption, EDR sensor, „relay” *(update server”);*<br>• Exista posibilitatea de instalare manuală, sau automată la distanţă, direct din consola de management;<br>• Din consola este disponibila informaţii despre fiecare endpoint: numele, IP, sistem de operare, module instalate, politica aplicată, informaţii despre actualizări;<br>• Posibilitatea de creare kit pentru endpoint – tip: universar – 32/64bit, fizic/VDI, web installe/full;<br>• Gestionare, creare şi configurare grupuri pentru endpoint ce nu sunt în AD; | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | ***b)*** *alternativă pentru fişierele infectate: interzice accesul, dezinfectează, ştergere, permutare fişiere în carantină;*<br>***c)*** *acţiune implicită pentru fişierele suspecte: interzice accesul, ştergere, mută fişierele în carantină, nici o acţiune;*<br>***d)*** *acţiune alternativă pentru fişierele suspecte: interzice accesul, ştergere, mută fişierele în carantină;*<br>• Scanarea automată în timp real cu setarea excepţiilor, definirea unor liste de excludere de la scanarea în timp real şi la cerere a anumitor directoare, discuri, fişiere, extensii sau procese, să nu scaneze arhive sau fişiere mai mari de ” x” MB, definirea nivelelor de profunzime pentru scanarea în arhive;<br>• Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicaţii cu potenţial periculos | • Posibilitate de atribuire a funcţionalităţii de descoperire a endpointurilor şi în afara AD, pentru oricare endpoint.<br>***<u>Caracteristici şi funcţionalităţi principale ale modulului antivirus:</u>***<br>Produsul permite:<br>• Stabilirea acţiunilor întreprinse de modulul antivirus la detectarea unei ameninţări noi. Astfel administratorul va putea alege între următoarele acţiuni:<br>***e)*** *implicită pentru fişiere infectate: interzice accesul, dezinfectează, ştergere, mută fişierele în carantină, nici o acţiune;*<br>***f)*** *alternativă pentru fişierele infectate: interzice accesul, dezinfectează, ştergere, permutare fişiere în carantină;*<br>***g)*** *acţiune implicită pentru fişierele suspecte: interzice accesul, ştergere, mută fişierele în carantină, nici o acţiune;* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă;<br>• Scanarea oricărui suport de stocare a informației *(CD-uri, harduri externe, unități partajate etc);*<br>• Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP;<br>• Configurarea căilor ce urmează a fi scanate la cerere;<br>• Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware;<br>• Setarea priorităților scanărilor programate;<br>• Soluția trebuie să permită configurarea mecanismelor de scanare utilizând tehnologii locale, bazate pe cloud sau alte mecanisme echivalente oferite de producător, pentru optimizarea performanței și consumului de resurse; | ***h)*** *acțiune alternativă pentru fișierele suspecte: interzice accesul, ștergere, mută fișierele în carantină;*<br>• Scanarea automată în timp real cu setarea excepțiilor, definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, extensii sau procese, să nu scaneze arhive sau fișiere mai mari de ”x” MB, definirea nivelelor de profunzime pentru scanarea în arhive;<br>• Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejând sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă;<br>• Scanarea oricărui suport de stocare a informației *(CD-uri, harduri externe, unități partajate etc);* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Administratorul trebuie să poată configura politicile şi mecanismele de scanare disponibile, inclusiv utilizarea tehnologiilor locale, bazate pe cloud sau a altor mecanisme echivalente, în funcţie de infrastructura protejată şi recomandările producătorului;<br>• Setarea a tipurilor de detecţie: bazate pe semnături, bazate de comportamentul fişierelor şi bazate pe monitorizarea proceselor;<br>• Scanarea paginilor web;<br>• Setarea a unei parole pentru protecţia la dezinstalare;<br>• Modul de antiphishing;<br>• Protecţie în timp real pe maşinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată;<br>• Soluţia trebuie să suporte implementarea în medii VDI persistente şi non-persistente, inclusiv utilizarea imaginilor de referinţă *(Golden Image/Template)* sau a unor mecanisme echivalente oferite de producător; | • Scanarea automată a emailurilor la nivelul staţiei de lucru pentru POP3/SMTP;<br>• Configurarea căilor ce urmează a fi scanate la cerere;<br>• Cu ajutorul unei baze de date complete cu semnături de spyware şi a euristicii de detecţie a acestui tip de programe, produsul va trebui să ofere protecţie anti-spyware;<br>• Setarea priorităţilor scanărilor programate;<br>• Soluţia permite configurarea mecanismelor de scanare utilizând tehnologii locale, bazate pe cloud sau alte mecanisme echivalente oferite de producător, pentru optimizarea performanţei şi consumului de resurse;<br>• Administratorul poate configura politicile şi mecanismele de scanare disponibile, inclusiv utilizarea tehnologiilor locale, bazate pe cloud sau a altor mecanisme echivalente, în funcţie de infrastructura protejată şi recomandările producătorului; | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Utilizarea uni modul adiţional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze şi blocheze atacuri de tip persistent sau targetat precum şi alte categorii de malware sofisticat înainte de faza de execuţie. Acest modul oferă următoarele funcţionalităţi:<br>***a)*** *clasificarea tipului de atac;*<br>***b)*** *abilitatea de a configura acţiunile aplicate ameninţărilor detectate, inclusiv raportarea, monitorizarea sau blocarea acestora;*<br>***c)*** *abilitatea de a configura nivelul de sensibilitate al mecanismelor de detecţie şi politicilor de securitate, conform recomandărilor producătorului;*<br>***d)*** *abilitatea de a acţiona în mod diferit în funcţie de tipul ameninţării (fişier sau atac prin reţea);* | • Setarea a tipurilor de detecţie: bazate pe semnături, bazate de comportamentul fişierelor şi bazate pe monitorizarea proceselor;<br>• Scanarea paginilor web;<br>• Setarea a unei parole pentru protecţia la dezinstalare;<br>• Modul de antiphishing;<br>• Protecţie în timp real pe maşinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată;<br>• Soluţia trebuie să suporte implementarea în medii VDI persistente şi non-persistente, inclusiv utilizarea imaginilor de referinţă *(Golden Image/Template)* sau a unor mecanisme echivalente oferite de producător;<br>• Utilizarea uni modul adiţional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze şi blocheze atacuri de tip persistent sau targetat precum şi alte categorii de | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Posibilitatea de restaurare a fişierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, cînd determină că procesul este maliţios;<br>• Oprirea atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive;<br>• Depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare;<br>• Protejarea aplicaţiilor utilizate frecvent şi a celor de tip „sistem" cum ar fi browserele, aplicaţiile de tip office sau reader, procesele critice aferente sistemelor de operare.<br><br>***<u>Firewall:</u>***<br><br>• Sa ofere posibilitatea de a configura reguli de firewall pentru aplicaţii sau conectivitate;<br>• Modulul să poată fi instalat/ activat/ dezactivat/ dezinstalat la cerere; | malware sofisticat înainte de faza de execuţie. Acest modul oferă următoarele funcţionalităţi:<br>***e)*** *clasificarea tipului de atac;*<br>***f)*** *abilitatea de a configura acţiunile aplicate ameninţărilor detectate, inclusiv raportarea, monitorizarea sau blocarea acestora;*<br>***g)*** *abilitatea de a configura nivelul de sensibilitate al mecanismelor de detecţie şi politicilor de securitate, conform recomandărilor producătorului;*<br>***h)*** *abilitatea de a acţiona în mod diferit în funcţie de tipul ameninţării (fişier sau atac prin reţea);*<br><br>• Posibilitatea de restaurare a fişierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Să permită definirea de reţele de încredere pentru maşina destinaţie.<br><br>***<u>Protecţia datelor:</u>***<br><br>• Produsul trebuie să permite blocarea datelor confidenţiale *(pin-ul cardului, cont bancar etc)* transmise prin HTTP sau SMTP prin crearea unor reguli specifice.<br>*[Raspuns clarificare (5 aug 2026, 10:19) În urma analizei observaţiilor primite, Autoritatea Contractantă constată că funcţionalităţile de prevenire a scurgerilor de date (DLP) reprezintă o categorie distinctă de soluţii, diferită de funcţionalităţile standard de protecţie a endpoint-urilor. Pentru a asigura o concurenţă cât mai largă şi pentru a evita restricţionarea nejustificată a participării operatorilor economici, cerinţa privind blocarea transmiterii datelor confidenţiale prin HTTP şi SMTP va fi exclusă din caietul de sarcini.]* | cînd determină că procesul este maliţios;<br>• Oprirea atacurile avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive;<br>• Depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare;<br>• Protejarea aplicaţiilor utilizate frecvent şi a celor de tip „sistem” cum ar fi browserele, aplicaţiile de tip office sau reader, procesele critice aferente sistemelor de operare.<br><br>***<u>Firewall:</u>***<br><br>• Ofera posibilitatea de a configura reguli de firewall pentru aplicaţii sau conectivitate;<br>• Modulul poate fi instalat/ activat/ dezactivat/ dezinstalat la cerere;<br>• Permite definirea de reţele de încredere pentru maşina destinaţie. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | *[Raspuns clarificare (6 aug 2026, 10:52): În cadrul prezentei proceduri de achiziție nu se stabilesc cerințe privind implementarea mecanismelor de blocare sau de mascarea a datelor confidențiale. Cerința referitoare la blocarea transmiterii datelor confidențiale prin intermediul protocoalelor HTTP și SMTP va fi exclusă din caietul de sarcini.]*<br><br>***<u>Controlul conținutului:</u>***<br><br>Produsul trebuie să ofere un modul integrat dedicat controlului accesului la Internet cu următoarele particularități: blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conțin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicații definite de administrator, restricționarea accesului pe | ***<u>Protecția datelor:</u>***<br><br>• Blocarea datelor confidențiale *(pin-ul cardului, cont bancar etc)* transmise prin HTTP sau SMTP prin crearea unor reguli specifice.<br>*[Raspuns clarificare (5 aug 2026, 10:19) În urma analizei observațiilor primite, Autoritatea Contractantă constată că funcționalitățile de prevenire a scurgerilor de date (DLP) reprezintă o categorie distinctă de soluții, diferită de funcționalitățile standard de protecție a endpoint-urilor. Pentru a asigura o concurență cât mai largă și pentru a evita restricționarea nejustificată a participării operatorilor economici, cerința privind blocarea transmiterii datelor confidențiale prin HTTP și SMTP va fi exclusă din caietul de sarcini.]*<br>*[Raspuns clarificare (6 aug 2026, 10:52): În cadrul prezentei proceduri de achiziție nu se stabilesc cerințe privind* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | anumite pagini de internet după anumite categorii prestabilite *(ex: online dating, violenta, pornografie etc).*<br><br>***<u>Controlul dispozitivelor:</u>***<br><br>Produsul trebuie să conţină un modul pentru controlul dispozitivelor care:<br>• Poate fi instalat/dezinstalat conform setărilor stabilite;<br>• Permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage;<br>• Permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la maşina client;<br>• Permite configurarea de excluderi pentru diferite tipuri | *implementarea mecanismelor de blocare sau de mascarea a datelor confidenţiale. Cerinţa referitoare la blocarea transmiterii datelor confidenţiale prin intermediul protocoalelor HTTP şi SMTP va fi exclusă din caietul de sarcini.]*<br><br>***<u>Controlul conţinutului:</u>***<br><br>Produsul ofera un modul integrat dedicat controlului accesului la Internet cu următoarele particularităţi: blocarea accesului la Internet pentru anumite maşini client sau grupuri de maşini, blocarea accesului la Internet pe intervale orare, blocarea paginilor de internet care conţin anumite cuvinte cheie, controlul accesului numai la anumite pagini de internet specificate de administrator, blocarea accesului la anumite aplicaţii definite de administrator, restricţionarea accesului pe anumite pagini de internet după anumite categorii | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | de dispozitive pentru care s-au configurat reguli.<br><br>***<u>Power User:</u>***<br><br>Produsul trebuie să conțină un modul pentru setări specifice – power user care să:<br>• Poată fi instalat/dezinstalat în funcție de preferința administratorului;<br>• Permită posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client;<br>• Permită administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User.<br>*[Raspuns clarificare (5 aug 2026, 10:23): Prin funcționalitatea „Power User" se înțelege posibilitatea acordării anumitor administratori a dreptului de a modifica local setările produsului de securitate după efectuarea unei autentificări suplimentare* | prestabilite *(ex: online dating, violenta, pornografie etc).*<br><br>***<u>Controlul dispozitivelor:</u>***<br><br>Produsul conține un modul pentru controlul dispozitivelor care:<br>• Poate fi instalat/dezinstalat conform setărilor stabilite;<br>• Permite controlul următoarelor tipuri de dispozitive: Bluetooth Devices, CDROM Devices, Floppy Disk Drives, Security Policies 153, IEEE 1284.4, IEEE 1394, Imaging Devices, Modems, Tape Drives, Windows Portable, COM/LPT Ports, SCSI Raid, Printers, Network Adapters, Wireless Network Adapters, Internal and External Storage;<br>• Permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client;<br>• Permite configurarea de excluderi pentru diferite tipuri | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | *(mod special sau credențiale dedicate). Acest mod trebuie să permită modificarea parametrilor care, în mod normal, sunt protejați prin politici centralizate și nu pot fi modificați local. ]*<br>*[Raspuns clarificare (5 aug 2026, 10:24): Prin funcționalitatea „Power User" se înțelege posibilitatea acordării anumitor administratori a dreptului de a modifica local setările produsului de securitate după efectuarea unei autentificări suplimentare (mod special sau credențiale dedicate). Acest mod trebuie să permită modificarea parametrilor care, în mod normal, sunt protejați prin politici centralizate și nu pot fi modificați local.]*<br><br>***<u>Actualizare:</u>***<br><br>Produsul trebuie să ofere posibilitatea de efectuare a actualizărilor:<br>• La nivel de stație în mod silențios *(fără avertizări);*<br>• Folosind unul sau mai multe servere de actualizare; | de dispozitive pentru care s-au configurat reguli.<br><br>***<u>Power User:</u>***<br><br>Produsul conține un modul pentru setări specifice – power user care să:<br>• Poate fi instalat/dezinstalat în funcție de preferința administratorului;<br>• Permite posibilitatea de a acorda utilizatorilor drepturi de Power User, pentru a putea accesa și modifica setările clientului antivirus dintr-o consola disponibilă local pe mașina client;<br>• Permite administratorului soluției să suprascrie din consola setările aplicate de utilizatorii Power User.<br>*[Raspuns clarificare (5 aug 2026, 10:23): Prin funcționalitatea „Power User" se înțelege posibilitatea acordării anumitor administratori a dreptului de a modifica local setările produsului de securitate* | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | • Pentru locațiile la distanță prin intermediul unui client antivirus care are și rol de server de actualizare.<br>• Gestionabil – doar local sau și servere online.<br><br>***<u>Protecție Anti-Tampering:</u>***<br><br>• Va permite detecția driverelor vulnerabile pe dispozitivele conectate *(endpointuri)* și când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrității produsului;<br>• Va permite detectarea de drivere vulnerabile pe dispozitivele conectate care pot fi exploatate de atacatori, reprezentând amenințări la adresa integrității produsului. Tehnologia este compatibilă cu sistemele de operare Windows și Linux;<br>• Va fi capabilă să protejeze împotriva amenințărilor noi sau erorilor umane neintenționate ce ar putea fi proiectate pentru a | *după efectuarea unei autentificări suplimentare (mod special sau credențiale dedicate). Acest mod trebuie să permită modificarea parametrilor care, în mod normal, sunt protejați prin politici centralizate și nu pot fi modificați local. ]*<br>*[Raspuns clarificare (5 aug 2026, 10:24): Prin funcționalitatea „Power User” se înțelege posibilitatea acordării anumitor administratori a dreptului de a modifica local setările produsului de securitate după efectuarea unei autentificări suplimentare (mod special sau credențiale dedicate). Acest mod trebuie să permită modificarea parametrilor care, în mod normal, sunt protejați prin politici centralizate și nu pot fi modificați local.]*<br><br>***<u>Actualizare:</u>*** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | permite acces neautorizat la kernel, ducând la compromiterea integrității poate detecta când funcțiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod malițios.<br><br>***<u>Disk Encryption:</u>***<br><br>Soluție pentru managementul criptării discurilor pentru 1000 entități.<br>Soluția va oferi următoarele funcționalități minime:<br><br>• Administrarea produsului trebuie să fie realizată din aceeaşi consolă de management ca şi soluția de protecție antivirus;<br>• Produsul va utiliza mecanismul nativ de criptare al sistemului de operare: BitLocker pentru Windows şi FileVault pentru Mac OSX;<br>*[Raspuns clarificare (5 aug 2026, 10:19) Se acceptă utilizarea unor tehnologii echivalente de criptare completă a discului, cu condiția ca acestea să asigure un nivel de securitate comparabil, administrare centralizată,* | Produsul ofera posibilitatea de efectuare a actualizărilor:<br>• La nivel de staţie în mod silenţios *(fără avertizări);*<br>• Folosind unul sau mai multe servere de actualizare;<br>• Pentru locațiile la distanță prin intermediul unui client antivirus care are şi rol de server de actualizare.<br>• Gestionabil – doar local sau şi servere online.<br><br>***<u>Protecție Anti-Tampering:</u>***<br><br>• Produsul permite detecția driverelor vulnerabile pe dispozitivele conectate *(endpointuri)* şi când sunt efectuate încercări avansate de atac pentru a dezactiva agentul de securitate, ceea ce poate duce la compromiterea integrității produsului;<br>• Permite detectarea de drivere vulnerabile pe dispozitivele conectate care pot fi exploatate de atacatori, reprezentând amenințări la adresa integrității produsului. | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | *recuperarea securizată a cheilor şi funcţionalităţi de monitorizare şi raportare. Utilizarea BitLocker şi FileVault nu este obligatorie, dacă soluţia propusă oferă funcţionalităţi echivalente. ]*<br>• Va asigura vizibilitatea completă asupra stării de criptare a dispozitivelor inclusiv: numele staţiei, IP-ul staţiei, sistemul de operare, ID-ul volumului/partiţiei, numele partiţiei, starea criptării partiţiei, tipul partiţiei: boot, non-boot, mărimea partiţiei în GB, ID-ul cheii de recuperare;<br>• Produsul trebuie să asigure criptarea pentru Următoarele OS: Windows 7/10/11 Pro/Enterprise *(with TPM)*; WindowsServer 2012/2012 R2, 2016, 2019, 2022 *(with TPM)*, OSX de la 10.12.<br><br>**<u>Alte cerinţe:</u>**<br>Perioada de suport şi menţinere de la producător:<br>**1.** Pentru soluţia ofertată se solicită a fi 36 luni; | Tehnologia este compatibilă cu sistemele de operare Windows şi Linux;<br>• Este capabil să protejeze împotriva ameninţărilor noi sau erorilor umane neintenţionate ce ar putea fi proiectate pentru a permite acces neautorizat la kernel, ducând la compromiterea integrităţii poate detecta când funcţiile de tip callback ale agentului de securitate au fost eliminate sau dezactivate în mod maliţios.<br><br>***<u>Disk Encryption:</u>***<br>Soluţia ESET PROTECT Enterprise On-prem/100 obj./3years include managementul criptării discurilor pentru 1000 entităţi.<br>Soluţia ofera următoarele funcţionalităţi minime:<br>• Administrarea produsului poate fi realizată din aceeaşi consolă de management ca şi soluţia de protecţie antivirus;<br>• Produsul utilizeaza mecanisme de criptare al | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | **2.** Producătorul trebuie să ofere suport 24/24, prin e-mail sau conectare de la distanţă.<br><br>***<u>Notă</u>:*** *Lucrările de instalare, configurare, punerea în funcţiune a soluţiei trebuie să fie executate de Ofertant, iar costul acestora trebuie să fie incluse în ofertă.* | sistemului de operare: Windows şi pentru Mac OSX; *[Raspuns clarificare (5 aug 2026, 10:19) Se acceptă utilizarea unor tehnologii echivalente de criptare completă a discului, cu condiţia ca acestea să asigure un nivel de securitate comparabil, administrare centralizată, recuperarea securizată a cheilor şi funcţionalităţi de monitorizare şi raportare. Utilizarea BitLocker şi FileVault nu este obligatorie, dacă soluţia propusă oferă funcţionalităţi echivalente. ]*<br>• Produsul asigura vizibilitatea completă asupra stării de criptare a dispozitivelor inclusiv: numele staţiei, IP-ul staţiei, sistemul de operare, ID-ul volumului/partiţiei, numele partiţiei, starea criptării partiţiei, tipul partiţiei: boot, non-boot, mărimea partiţiei în GB, ID-ul cheii de recuperare;<br>• Produsul asigura criptarea pentru Următoarele | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | OS: Windows 7/10/11 Pro/Enterprise *(with TPM)*; WindowsServer 2012/2012 R2, 2016, 2019, 2022 *(with TPM)*, OSX de la 10.12.<br><br>**<u>Alte cerinţe:</u>**<br><br>Perioada de suport şi menţinere de la producător:<br>**1.** Pentru soluţia ofertată perioada de suport şi menţinere de la producător este de 36 luni;<br>**2.** Producătorul ofera suport 24/24, prin e-mail sau conectare de la distanţă.<br><br>***<u>Notă</u>:*** *Lucrările de instalare, configurare, punerea în funcţiune a soluţiei vor fi executate de S.R.L. "KOMPASS MOLDOVA", iar costul acestora este inclus în ofertă.* | |

Numele, prenumele: **Latii Iurie**
În calitate de: **Director**
Ofertantul: **S.R.L. "KOMPASS MOLDOVA"**
Adresa: str. N. Zelinski, 36/8, ap.(of.) 23

Digitally signed by Latii Iurie
Date: 2026.08.11 16:09:57 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ