

“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

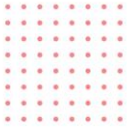
str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

Anexa nr. 23
la Documentația standard aprobată
prin Ordinul Ministrului Finanțelor nr. 115 din 15.09.2021

Specificații tehnice

Numărul procedurii de achiziție: ocds-b3wdp1-MD-1666186160753 din 19 octombrie 2022						
Obiectul achiziției: Servicii informatice de securitate antivirus pentru protecția infrastructurii IT						
Denumirea bunurilor	Denumirea modelului bunului/serviciului	Țara de origine	Producătorul	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 1: Servicii informatice de securitate antivirus pentru protecția infrastructurii IT						
Servicii informatice de securitate antivirus pentru protecția infrastructurii IT	Bitdefender GravityZone Business Security Enterprise, 150 users, 36 luni	Romania	Bitdefender	Specificația serviciilor informatice de securitate antivirus pentru protecția infrastructurii IT: Se solicita achiziția a unei soluții corporative de tip anti-malware, care să ofere protecție, securitatea și scanarea vulnerabilităților a 150 de stații de lucru, servere fizice și virtualizate, cutii poștale pentru o perioadă de 36 luni. Produsul (soluția) să reprezinte o platformă integrată pentru managementul securității, gândită ca o soluție modulară. Produsul trebuie să conțină următoarele module:	Specificația serviciilor informatice de securitate antivirus pentru protecția infrastructurii IT oferată: Se oferă soluția <u>Bitdefender GravityZone Business Security Enterprise</u> ; soluție corporativă de tip anti-malware, oferă protecție, securitatea și scanarea vulnerabilităților a 150 de stații de lucru, servere fizice și virtualizate, cutii poștale pentru o perioadă de 36 luni. Produsul (soluția) reprezintă o platformă integrată pentru managementul securității, gândită ca o soluție modulară. Produsul conține următoarele	-



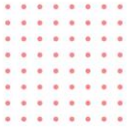
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			1. Consola de management care asigura funcționalități de administrare. 2. Protecție stații și servere fizice/virtuale. 3. Protecție și securitate pentru serverele email Microsoft Exchange 1. CONSOLA DE MANAGEMENT 1.1 Instalare și configurare: 1.1.1. Pachetul de instalare necesar să fie livrat ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Consola nu va necesita olicenta suplimentara pentru sistemul de operare. Imaginea de tip template trebuie să se poată importa în Microsoft Hyper-V 1.1.2. Soluția să fie scalabilă, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași masina virtuală. 1.1.3. Soluția este necesar să includă aditional și un modul de balansare (load balancer) pentru cazurile în care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru Load Balancing și performanta/redundanta). 1.2 Cerinte generale: 1.2.1. Produsul trebuie să suporte licențierea per procesor fizic (socket). în felul acesta numărul	module: 1. Consola de management asigură funcționalități de administrare. 2. Protecție stații și servere fizice/virtuale. 3. Protecție și securitate pentru serverele email Microsoft Exchange 1. CONSOLA DE MANAGEMENT 1.1 Instalare și configurare: 1.1.1. Pachetul de instalare va fi livrat ca o masina virtuala bazata pe sistem de operare Linux securizat care contine toate rolurile sau serviciile necesare. Consola nu necesita o licenta suplimentara pentru sistemul de operare. Imaginea de tip template poate importa în Microsoft Hyper-V 1.1.2. Soluția este scalabilă, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași masina virtuală. 1.1.3. Soluția include aditional și un modul de balansare (load balancer) pentru cazurile în care mai multe mașini virtuale ale componentei de management sunt instalate cu același rol (pentru Load Balancing și performanta/redundanta). 1.2 Cerinte generale: 1.2.1. Produsul suportă licențierea per procesor fizic (socket). în felul acesta numărul	
--	--	--	---	---	--





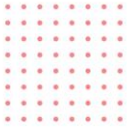
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

				mașinilor virtuale poate varia oricând, ele fiind protejate. 1.2.2. Soluția trebuie să includă un modul de update server prin care se asigură actualizarea de produs și a semnatuurilor. 1.2.3. Soluția trebuie să permită activarea/dezactivarea actualizărilor de produs/semnături. 1.2.4. Soluția trebuie să permită stabilirea actualizării automate a consolei de management prin stabilirea recurenței zilnice, săptămânale sau lunare, dar și prin stabilirea intervalului orar în care acesta se va actualiza. De asemenea, permite și trimiterea unei alerte de nefuncționalitate, cu 30 de minute înainte de actualizare. 1.2.5. Notificările – prezente în interfața, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de produs disponibile). 1.2.6. Soluția trebuie să permită instalarea serviciului de SMNP prin care se pot raporta statusul mașinilor din cadrul componentei de management. 1.2.7. Soluția trebuie să permită crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programată, putând fi stocată	mașinilor virtuale poate varia oricând, ele fiind protejate. 1.2.2. Soluția include un modul de update server prin care se asigură actualizarea de produs și a semnatuurilor. 1.2.3. Soluția permite activarea/dezactivarea actualizărilor de produs/semnături. 1.2.4. Soluția permite stabilirea actualizării automate a consolei de management prin stabilirea recurenței zilnice, săptămânale sau lunare, dar și prin stabilirea intervalului orar în care acesta se va actualiza. De asemenea, permite și trimiterea unei alerte de nefuncționalitate, cu 30 de minute înainte de actualizare. 1.2.5. Notificările – prezente în interfața, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de produs disponibile). 1.2.6. Soluția permite instalarea serviciului de SMNP prin care se pot raporta statusul mașinilor din cadrul componentei de management. 1.2.7. Soluția permite crearea unei copii de siguranță a bazei de date a consolei de administrare, la cerere sau programată, putând fi stocată local, pe un server FTP sau în rețea.	
--	--	--	--	---	--	--





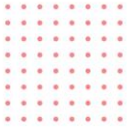
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

				local, pe un server FTP sau în rețea. 1.3 Panou de monitorizare și raportare (Dashboard): 1.3.1. Rapoartele din panoul de monitorizare necesar să fie posibil configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport. 1.3.2. Panoul central necesar să contine rapoarte pentru toate modulele suportate. 1.4 Inventarierea rețelei – managementul securității: 1.4.1. Soluția să fie integrată cu domenii Active Directory multiple, și importa inventarul acestor platforme. 1.4.2. Soluția trebuie să permită descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. 1.4.3. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare, adresa IP, politica aplicată, ultima dată când s-a conectat (online și/sau offline) și FQDN. 1.4.4. Soluția trebuie să permită crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care	1.3 Panou de monitorizare și raportare (Dashboard): 1.3.1. Rapoartele din panoul de monitorizare pot fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport. 1.3.2. Panoul central contine rapoarte pentru toate modulele suportate. 1.4 Inventarierea rețelei – managementul securității: 1.4.1. Soluția poate fi integrată cu domenii Active Directory multiple, și importa inventarul acestor platforme. 1.4.2. Soluția permite descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. 1.4.3. Soluția ofera opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare, adresa IP, politica aplicată, ultima dată când s-a conectat (online și/sau offline) și FQDN. 1.4.4. Soluția permite crearea unui pachet unic pentru toate sistemele de operare, de stații sau servere. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care ruleaza	
--	--	--	--	--	---	--





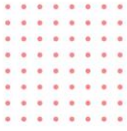
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

				ruleaza sistemul de operare Windows, Linux, 1.4.5. Soluția trebuie să permită instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale. 1.4.6. Soluția trebuie să permită selectarea modulelor componente atunci când se crează pachetul clientului care se instalează pe mașinile fizice/virtuale. 1.4.7. Soluția trebuie să permită lansarea de task-uri de scanare, actualizare, instalare, deinstalare la distanță pentru clientul antimalware. 1.4.8. Soluția trebuie să ofere posibilitatea de repornire a mașinilor fizice de la distanță. 1.4.9. Soluția trebuie să ofere informații detaliate despre fiecare task și se fiseaza daca task-ul s-a finalizat sau nu cu succes. 1.4.10. Soluția trebuie să permită configurarea centralizată a clienților antimalware prin intermediul politicilor 1.4.11. Soluția trebuie să ofere în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.	sistemul de operare Windows, Linux. 1.4.5. Soluția permite instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale. 1.4.6. Soluția permite selectarea modulelor componente atunci când se crează pachetul clientului care se instalează pe mașinile fizice/virtuale. 1.4.7. Soluția permite lansarea de task-uri de scanare, actualizare, instalare, deinstalare la distanță pentru clientul antimalware. 1.4.8. Soluția oferă posibilitatea de repornire a mașinilor fizice de la distanță. 1.4.9. Soluția oferă informații detaliate despre fiecare task și se fiseaza daca task-ul s-a finalizat sau nu cu succes. 1.4.10. Soluția permite configurarea centralizată a clienților antimalware prin intermediul politicilor 1.4.11. Soluția oferă în consola de management informații detaliate ale obiectelor din consola: Nume, IP, Sistem de operare, Grup, Politica atribuita, Ultimele actualizare, Versiunea produsului, Versiunea de semnături.	
--	--	--	--	--	---	--





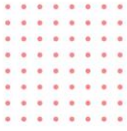
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			1.4.12. Pentru integrarea cu Active Directory, se va putea defini și intervalul (în ore) de sincronizare 1.4.13. Soluția trebuie să permită descoperirea mașinilor din Microsoft Hyper-V 1.4.14. Soluția trebuie să permită descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare. 1.5 Politici: 1.5.1. Soluția trebuie să permită configurarea setărilor clientului antimalware prin intermediul unei singure politici ce conține setări pentru toate modulele. 1.5.2. Politica să conțină opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user. 1.5.3. Soluția trebuie să permită aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unitati organizationale, grupuri de securitate sau useri de active directoy. 1.5.4. Politica să poata fi schimbata automat în functie de: • IP sau clasa de IP al stației • Gateway-ul alocat	1.4.12. Pentru integrarea cu Active Directory, se va putea defini și intervalul (în ore) de sincronizare 1.4.13. Soluția permite descoperirea mașinilor din Microsoft Hyper-V 1.4.14. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare. 1.5 Politici: 1.5.1. Soluția permite configurarea setărilor clientului antimalware prin intermediul unei singure politici ce conține setări pentru toate modulele. 1.5.2. Politica conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, controlul aplicațiilor, scanarea traficului web, controlul dispozitivelor, power user. 1.5.3. Soluția permite aplicarea politicilor pe mașini client, grupuri de mașini, pool-uri de resurse (VMware), domeniu, unitati organizationale, grupuri de securitate sau useri de active directoy. 1.5.4. Politica poate fi schimbata automat în functie de: • IP sau clasa de IP al stației • Gateway-ul alocat	
--	--	--	--	--	--





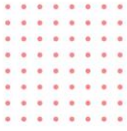
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			• DNS serverul alocat • WINS serverul alocat • Sufix DNS pentru conexiunea dhcp • Clientul este/nu este în aceeași rețea cu infrastructura de management (stația de lucru poate soluționa implicit numele gazdei) • Tipul rețelei (lan, wireless) • User-ul logat pe stație 1.6 Rapoarte: 1.6.1. Soluția trebuie să conțină rapoarte care prezintă statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate. 1.6.2. Soluția trebuie să permită vizualizarea rapoartelor curente programate de administrator. 1.6.3. Soluția trebuie să permită exportarea rapoartelor în format .pdf și detaliile ca format .csv. 1.6.4. Soluția trebuie să permită filtrarea informațiilor continute în rapoartele trimise pe mail astfel încât doar informațiile relevante cerute de către administrator vor fi transmise pe email. 1.6.5. Soluția trebuie să includă un generator de rapoarte care oferă posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate	• DNS serverul alocat • WINS serverul alocat • Sufix DNS pentru conexiunea dhcp • Clientul este/nu este în aceeași rețea cu infrastructura de management (stația de lucru poate soluționa implicit numele gazdei) • Tipul rețelei (lan, wireless) • User-ul logat pe stație 1.6 Rapoarte: 1.6.1. Soluția conține rapoarte care prezintă statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate. 1.6.2. Soluția permite vizualizarea rapoartelor curente programate de administrator. 1.6.3. Soluția permite exportarea rapoartelor în format .pdf și detaliile ca format .csv. 1.6.4. Soluția permite filtrarea informațiilor continute în rapoartele trimise pe mail astfel încât doar informațiile relevante cerute de către administrator vor fi transmise pe email. 1.6.5. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problemă de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate	
--	--	--	--	---	--





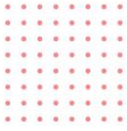
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

				corespunzator. Astfel, soluția include interogari precum: starea terminalului, evenimente terminal, evenimente Exchange. 1.6.6. Interogarea legata de starea terminalului include informații precum: • tip masina • infrastructura rețelei căreia îi aparține terminalul • datele agentului de securitate • starea modulelor de protecție • rolurile terminalelor. 1.6.7. Interogarea legată de evenimente terminal include informații precum: • calculatorul ținta pe care a avut loc evenimentul • tipul starea și configurația agentului de securitate instalat • starea modulelor și rolurilor de protecție instalate pe agentul de securitate • denunmirea și alocarea politicii • utilizatorul autentificat în timpul evenimentului • evenimente (site-uri blocate, aplicatii blocate, detectiile etc)	corespunzator. Astfel, soluția include interogari precum: starea terminalului, evenimente terminal, evenimente Exchange. 1.6.6. Interogarea legata de starea terminalului include informații precum: • tip masina • infrastructura rețelei căreia îi aparține terminalul • datele agentului de securitate • starea modulelor de protecție • rolurile terminalelor. 1.6.7. Interogarea legată de evenimente terminal include informații precum: • calculatorul ținta pe care a avut loc evenimentul • tipul starea și configurația agentului de securitate instalat • starea modulelor și rolurilor de protecție instalate pe agentul de securitate • denunmirea și alocarea politicii • utilizatorul autentificat în timpul evenimentului • evenimente (site-uri blocate, aplicatii blocate, detectiile etc)	
--	--	--	--	---	---	--





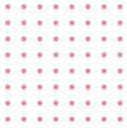
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			1.6.8. Interogarea legata de evenimente Exchange include informații precum: • Direcția traficului e-mail • Evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate) • Măsurile implementate în fiecare situație (curățarea, stergerea, înlocuirea sau carantinarea fișierului, stergerea sau respingerea e-mail-ului) 1.7 Carantina: 1.7.1. Soluția trebuie să permită restaurarea fișierelor carantinate în locația originală sau într-o cale configurabilă. 1.7.2. Carantina trebuie să sa fie locala, pe fiecare stația administrată și va fi administrată, fie local, fie din consola de management. 1.8 Utilizatori: 1.8.1. Administrarea trebuie să se poata face pe baza de roluri. 1.8.2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat. • Administrator companie: administreaza arhitectura consolei de management; • Administrator rețea: administreaza serviciile de securitate;	1.6.8. Interogarea legata de evenimente Exchange include informații precum: • Direcția traficului e-mail • Evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate) • Măsurile implementate în fiecare situație (curățarea, stergerea, înlocuirea sau carantinarea fișierului, stergerea sau respingerea e-mail-ului) 1.7 Carantina: 1.7.1. Soluția permite restaurarea fișierelor carantinate în locația originală sau într-o cale configurabilă. 1.7.2. Carantina este locală, pe fiecare stația administrată și va fi administrată, fie local, fie din consola de management. 1.8 Utilizatori: 1.8.1. Administrarea se poate face pe baza de roluri. 1.8.2. Roluri multiple predefinite: Administrator companie, Administrator rețea, Reporter sau rol personalizat. • Administrator companie: administreaza arhitectura consolei de management; • Administrator rețea: administreaza serviciile de securitate;	
--	--	--	--	---	--





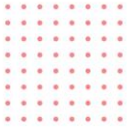
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			Reporter: monitorizeaza și generează rapoarte. 1.8.3. Utilizatorii pot fi importati din Microsoft Active Directory sau creati în consola de management. 1.8.4. Soluția trebuie să permită configurarea detaliată a drepturilor administrative, permitând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. 1.9 Log-uri: 1.9.1. Inregistrarea actiunilor utilizatorilor. 1.9.2. Sa fie oferite informații detaliate pentru fiecare actiune a unui utilizator. 1.9.3. Sa permită filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. 1.10 Actualizare: 1.10.1. Sa permită definirea de locatii de actualizare multiple. 1.10.2. Sa permită activarea/dezactivarea actualizarilor de produs și semnături. 1.10.3. Sa permită actualizarea produsului într-o rețea fără acces la Internet. 1.10.4. Soluția să dispuna un server de actualizare (update) care va face posibila stabilirea componentelor ce vor fi descarcate automat de pe internet, fără intervenția administratorului.	Reporter: monitorizeaza și generează rapoarte. 1.8.3. Utilizatorii pot fi importati din Microsoft Active Directory sau creati în consola de management. 1.8.4. Soluția permite configurarea detaliată a drepturilor administrative, permitând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. 1.9 Log-uri: 1.9.1. Inregistrarea actiunilor utilizatorilor. 1.9.2. Soluția oferă informații detaliate pentru fiecare actiune a unui utilizator. 1.9.3. Soluția permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. 1.10 Actualizare: 1.10.1. Soluția permite definirea de locatii de actualizare multiple. 1.10.2. Soluția permite activarea/dezactivarea actualizarilor de produs și semnături. 1.10.3. Soluția permite actualizarea produsului într-o rețea fără acces la Internet. 1.10.4. Soluția dispune de un server de actualizare (update) care va face posibila stabilirea componentelor ce vor fi descarcate automat de pe internet, fără intervenția administratorului.	
--	--	--	---	---	--





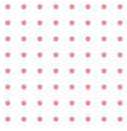
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			Astfel, administratorul va putea descarca pachetele pentru protecția stațiilor și serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac sau, poate descarca pachetele pentru modul de scanare centralizata în mediile de virtualizare Hyper-V. 1.10.5. Soluția să permită testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitand posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare să includa 2 tipuri de actualizări de produs: • Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei • Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc) 1.10.6. Soluția să permită stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management. 1.11 Certificate: 1.11.1. Accesul la consola de management să se faca doar prin HTTPS. 1.11.2. Serverul web, din consola centrala de management trebuie să permită importarea de certificate digitale eliberate de o autoritate de certificare autorizată sau proprie organizației.	Astfel, administratorul va putea descarca pachetele pentru protecția stațiilor și serverelor pe care ruleaza sistemul de operare Windows, Linux, Mac sau, poate descarca pachetele pentru modul de scanare centralizata în mediile de virtualizare Hyper-V. 1.10.5. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitand posibile probleme ce pot afecta serverele sau stațiile critice. Serverul de actualizare include 2 tipuri de actualizări de produs: • Ciclu rapid, gândit pentru un mediu de test în cadrul rețelei • Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc) 1.10.6. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management. 1.11 Certificate: 1.11.1. Accesul la consola de management se face doar prin HTTPS. 1.11.2. Serverul web, din consola centrala de management permite importarea de certificate digitale eliberate de o autoritate de	
--	--	--	---	---	--





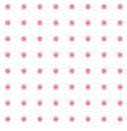
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			1.11.3. Soluția trebuie să permită afișarea în consola de management informații despre certificate: nume, autoritatea emitentă, data eliberării și data expirării certificatelor eliberate. 2. PROTECTIE STAȚII ȘI SERVERE FIZICE SAU VIRTUALE 2.1 Caracteristici generale minimale și eliminatorii: 2.1.1. Pentru reducerea la minim a consumului de resurse, soluția antimalware trebuie să permită instalarea personalizată a modulelor deținute (de exemplu, să permită instalarea soluției antimalware fara modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall). 2.1.2. Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includa un vaccin antiransomware. Acest vaccin asigura protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare. 2.1.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.	certificare autorizată sau proprie organizației. 1.11.3. Soluția permite afișarea în consola de management informații despre certificate: nume, autoritatea emitentă, data eliberării și data expirării certificatelor eliberate. 2. PROTECTIE STAȚII ȘI SERVERE FIZICE SAU VIRTUALE 2.1 Caracteristici generale minimale și eliminatorii: 2.1.1. Pentru reducerea la minim a consumului de resurse, soluția antimalware permite instalarea personalizată a modulelor deținute (de exemplu, permite instalarea soluției antimalware fara modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall). 2.1.2. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un vaccin antiransomware. Acest vaccin asigura protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare. 2.1.3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.	
--	--	--	--	--	--





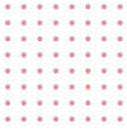
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			2.1.4. Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includă protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de învățare automată (machine learning). 2.1.5. Pentru o mai bună protecție a stațiilor și serverelor, soluția trebuie să includă un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil” proiectat special pentru a detecta atacuri avansate și activități suspecte în faza pre-executie. 2.1.6. Acest modul avansat de securitate va proteja împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecarui tip de amenințare menționat, i se vor putea stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv. 2.1.7. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecța, șterge sau muta în carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide dacă dorește întâi monitorizare sau dorește și blocarea amenințărilor. Aceste	2.1.4. Pentru o mai bună protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de învățare automată (machine learning). 2.1.5. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un modul avansat de securitate – HyperDetect, bazat pe tehnologii de tip „machine learning tunabil” proiectat special pentru a detecta atacuri avansate și activități suspecte în faza pre-executie. 2.1.6. Acest modul avansat de securitate va proteja împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecarui tip de amenințare menționat, i se vor putea stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv. 2.1.7. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecța, șterge sau muta în carantina pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide dacă dorește întâi monitorizare sau dorește și blocarea amenințărilor. Aceste acțiuni menționate, pot fi stabilite independent, pentru	
--	--	--	---	--	--





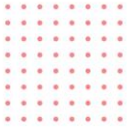
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

				acțiuni menționate, vor putea fi stabilite independent, pentru fișiere sau pentru traficul din rețea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenințările care ar fi fost detectate dacă nivelul de protecție era stabilit mai agresiv). 2.1.8. Pentru a oferi un nivel aditional de protecție a stațiilor și serverelor, soluția trebuie să includa un sandbox în cloud-ul public al producatorului acesteia. 2.1.9. Modulul de Sandbox va putea trimite automat fișiere în Sandbox-ul din cloud-ul producătorului unde vor putea fi „detonate” pentru o analiză în profunzime. 2.1.10. Modulul de Sandbox trebuie să includă două variante de analiză: doar monitorizare sau blocare. În modul monitorizare utilizatorul va putea accesa fișierul dorit, pe când în modul blocare, utilizatorului i se va bloca rularea fișierului până când Sandbox-ul din cloud-ul producatorului va da verdictul. 2.1.11. Modulul de Sandbox trebuie să includa doua tipuri de actiuni remediere: implicită și de siguranță. Pentru acțiunea implicită se va putea stabili: doar raportare, dezinfectie, stergere și	fișiere sau pentru traficul din rețea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenințările care ar fi fost detectate dacă nivelul de protecție era stabilit mai agresiv). 2.1.8. Pentru a oferi un nivel aditional de protecție a stațiilor și serverelor, soluția include un sandbox în cloud-ul public al producatorului Bitdefender. 2.1.9. Modulul de Sandbox poate trimite automat fișiere în Sandbox-ul din cloud-ul producătorului unde vor putea fi „detonate” pentru o analiză în profunzime. 2.1.10. Modulul de Sandbox include două variante de analiză: doar monitorizare sau blocare. În modul monitorizare utilizatorul va putea accesa fișierul dorit, pe când în modul blocare, utilizatorului i se va bloca rularea fișierului până când Sandbox-ul din cloud-ul producatorului va da verdictul. 2.1.11. Modulul de Sandbox include doua tipuri de actiuni remediere: implicită și de siguranță. Pentru acțiunea implicită se poate stabili: doar raportare, dezinfectie, stergere și carantinare. Pentru	
--	--	--	--	---	--	--





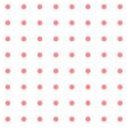
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			carantinare. Pentru actiunea de siguranta se va putea stabili: stergere sau carantinare. 2.1.12. Modulul de Sandbox trebuie să includă și posibilitatea de trimitere manuală a fișierelor în Sandbox-ul din cloud-ul producatorului. Astfel, daca administratorul suspecteaza un fisier ca fiind malițios, îl poate trimite manual în Sandbox pentru a fi „detonat” și a afla verdictul. Va putea trimite mai multe fișiere de odată, cu posibilitate de a specifica dacă vor fi „detonate” individual sau toate în acelasi timp. 2.1.13. Modulul de Sandbox poate suporta „detonarea” urmatoarelor tipuri de fisiere: 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. 2.1.14. Fișierele mentionate anterior, vor putea fi detectate corect chiar dacă sunt incluse în arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS	actiunea de siguranta se poate stabili: stergere sau carantinare. 2.1.12. Modulul de Sandbox include și posibilitatea de trimitere manuală a fișierelor în Sandbox-ul din cloud-ul producatorului. Astfel, daca administratorul suspecteaza un fisier ca fiind malițios, îl poate trimite manual în Sandbox pentru a fi „detonat” și a afla verdictul. Va putea trimite mai multe fișiere de odată, cu posibilitate de a specifica dacă vor fi „detonate” individual sau toate în acelasi timp. 2.1.13. Modulul de Sandbox poate suporta „detonarea” urmatoarelor tipuri de fisiere: 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. 2.1.14. Fișierele mentionate anterior, pot fi detectate corect chiar dacă sunt incluse în arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS	
--	--	--	--	--	--





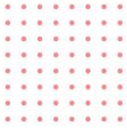
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ. 2.1.15. Modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response”) capabil să identifice amenințări avansate sau atacuri în curs de desfășurare. 2.1.16. Acest modul cuprinde colectare de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliată a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate - – HyperDetect. Din punct de vedere functional modulul EDR cuprinde 2 componente distincte: senzorul ce colectează și procesează datele respectiv partea de analiza de securitate care are ca obiect interpretarea acestora. 2.1.17. Modulul EDR trebuie să aiba capacitatea de a evalua activitatea tipică a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining”) și poate raporta orice deviație de la acest comportament sub forma unui incident	Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ. 2.1.15. Modul de detectare, corelare și răspuns la evenimente de tip EDR („endpoint detection and response”) capabil să identifice amenințări avansate sau atacuri în curs de desfășurare. 2.1.16. Acest modul cuprinde colectare de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliată a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de securitate - – HyperDetect. Din punct de vedere functional modulul EDR cuprinde 2 componente distincte: senzorul ce colectează și procesează datele respectiv partea de analiza de securitate care are ca obiect interpretarea acestora. 2.1.17. Modulul EDR are capacitatea de a evalua activitatea tipică a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining”) și poate raporta orice deviație de la acest comportament sub forma unui incident	
--	--	--	---	---	--





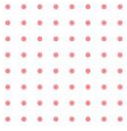
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			2.1.18. Modulul EDR trebuie să permită filtrarea incidentelor din interfata grafica în funcție intervalul de timp, pe baza unui scor de încredere („confidence score”), indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cât și după IP, nume fișier, nume stație. 2.1.19. Modulul EDR trebuie să permită vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat după cum urmează: tabul „rezumat” generează o hartă de principiu a incidentului, tabul „timeline” detaliază incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, respectiv butonul „acționează” care poate genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adaugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod). 2.1.20. Modulul EDR trebuie să poată bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV. 2.1.21. Modulul EDR trebuie să poată excepta fișiere non-malițioase de la acțiunea de	2.1.18. Modulul EDR trebuie să permită filtrarea incidentelor din interfata grafica în funcție intervalul de timp, pe baza unui scor de încredere („confidence score”), indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cât și după IP, nume fișier, nume stație. 2.1.19. Modulul EDR permite vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat după cum urmează: tabul „rezumat” generează o hartă de principiu a incidentului, tabul „timeline” detaliază incidentul în funcție de amprenta de timp a fiecărei acțiuni aferente incidentului, respectiv butonul „acționează” care poate genera un set de măsuri specifice fiecărui element din harta incidentului (kill, carantina – la nivel de nod, investigați – virus total, sandbox, google – la nivel de fișier, adaugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod). 2.1.20. Modulul EDR poate bloca fișiere și/sau procese folosind valori hash de tip MD5/SHA256 direct din pagina aferentă incidentului sau importate folosind un fișier CSV. 2.1.21. Modulul EDR poate excepta fișiere non-malițioase de la acțiunea de investigare	
--	--	--	---	--	--





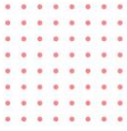
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			investigare sau poate genera/adauga un set de fișiere malițioase într-o lista neagra pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase. 2.1.22. Modulul EDR trebuie să permită deschiderea unei conexiuni remote catre un endpoint potential infectat pentru a permite o investigare rapida a gazdei, colecta date despre atac respectiv remedie în timp real brese de securitate eliminând astfel posibile incertitudini privitoare la comportamentul potential malițios al unor fișiere/procese, reducând timpul de remediere (downtime) în cazul în care un atac a avut succes și stația ținta trebuie reconfigurata/reinstalata, permite executarea unor comenzi în linia de comanda care se executa cu privilegii de kernel ce permit eliminarea în timp real a unor amenințari sau colectarea de date privitoare la atacul în desfășurare. 2.1.23. Modulul EDR trebuie să permită creare regulilor de detecție customizabile bazate pe procese, fișiere, registri și conexiuni de rețea. 2.1.24. Modulul EDR trebuie să permită creare regulilor de excludere customizabile bazate pe procese, fișiere, registri și conexiuni de rețea.	sau poate genera/adauga un set de fișiere malițioase într-o lista neagra pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase. 2.1.22. Modulul EDR permite deschiderea unei conexiuni remote catre un endpoint potential infectat pentru a permite o investigare rapida a gazdei, colecta date despre atac respectiv remedie în timp real brese de securitate eliminând astfel posibile incertitudini privitoare la comportamentul potential malițios al unor fișiere/procese, reducând timpul de remediere (downtime) în cazul în care un atac a avut succes și stația ținta trebuie reconfigurata/reinstalata, permite executarea unor comenzi în linia de comanda care se executa cu privilegii de kernel ce permit eliminarea în timp real a unor amenințari sau colectarea de date privitoare la atacul în desfășurare. 2.1.23. Modulul EDR permite creare regulilor de detecție customizabile bazate pe procese, fișiere, registri și conexiuni de rețea. 2.1.24. Modulul EDR permite creare regulilor de excludere customizabile bazate pe procese, fișiere, registri și conexiuni de rețea.	
--	--	--	---	--	--





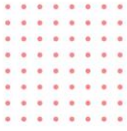
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			2.1.25. Modulul EDR trebuie să permită căutarea proactiva pe stațiile de lucru protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registri, valori de registri. 2.1.26. Soluția trebuie să includă un modul de tip host IPS capabil să blocheze atacuri la nivel de rețea incluzând mișcarea laterală a unor categorii de malware. 2.1.27. Modulul de tip host IPS va reprezenta o sursă de telemetrie / date despre atac pentru modulul de tip EDR, acesta din urma având abilitatea de a integra informații despre acțiunile luate de către o potențială amenințare la nivel de rețea. 2.2 Administrare și instalare remote: 2.2.1. Înainte de instalare, administratorul trebuie să poată particulariza pachetele de instalare cu modulele dorite 2.2.2. În consola vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc. 2.2.3. Din consola trebuie să se poată trimite o singură politică pentru configurarea integrală a clientului de pe stații/serve.	2.1.25. Modulul EDR permite căutarea proactiva pe stațiile de lucru protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de registri, valori de registri. 2.1.26. Soluția include un modul de tip host IPS capabil să blocheze atacuri la nivel de rețea incluzând mișcarea laterală a unor categorii de malware. 2.1.27. Modulul de tip host IPS reprezinta o sursă de telemetrie / date despre atac pentru modulul de tip EDR, acesta din urma are abilitatea de a integra informații despre acțiunile luate de către o potențială amenințare la nivel de rețea. 2.2 Administrare și instalare remote: 2.2.1. Înainte de instalare, administratorul poate particulariza pachetele de instalare cu modulele dorite 2.2.2. În consola sunt disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politica aplicata, informații despre actualizări etc. 2.2.3. Din consola se poate trimite o singură politică pentru configurarea integrală a clientului de pe stații/serve.	
--	--	--	--	---	--





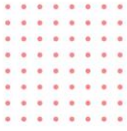
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			2.2.4. Consola trebuie să includă o secțiune, „Audit”, unde se vor menționa toate acțiunile întreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc. 2.2.5. Soluția trebuie să-i permită administratorului să poată crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/servelele din rețea pentru cele care nu sunt integrate în domeniu. 2.2.6. Soluția trebuie să permită selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu. 2.3 Caracteristici și funcționalități principale ale modulului antimalware: 2.3.1. Soluția să permită administratorului să stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni: - Acțiune implicită pentru fișiere infectate: • interzice accesul • dezinfectează • ștergere • mută fișierele în carantina • nicio acțiune	2.2.4. Consola include o secțiune, „Audit”, unde se vor menționa toate acțiunile întreprinse fie de administratori fie de reporteri, cu informații detaliate: logare, editare, creare, delogare, mutare etc. 2.2.5. Soluția îi permite administratorului să poată crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/servelele din rețea pentru cele care nu sunt integrate în domeniu. 2.2.6. Soluția permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decât cele integrate în domeniu. 2.3 Caracteristici și funcționalități principale ale modulului antimalware: 2.3.1. Soluția permite administratorului să stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul poate alege între următoarele acțiuni: - Acțiune implicită pentru fișiere infectate: • interzice accesul • dezinfectează • ștergere • mută fișierele în carantina • nicio acțiune	
--	--	--	--	--	--





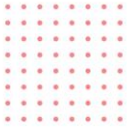
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			- Acțiune alternativă pentru fișierele infectate: • interzice accesul • dezinfectează • ștergere • muta fișierele în carantină - Acțiune implicită pentru fișierele suspecte: • interzice accesul • ștergere • muta fișierele în carantină • nicio acțiune - Acțiune alternativă pentru fișierele suspecte: • interzice accesul • ștergere • mută fișierele în carantină. 2.3.2. Scanarea automată în timp real va putea fi setată să nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor putând fi definită de administratorul soluției, 2.3.3. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP. 2.3.4. Clientii antimalware pentru workstation să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, certificate, extensii sau procese, incluzând amprenta (hash) în cazul fișierelor sau certificatelor.	- Acțiune alternativă pentru fișierele infectate: • interzice accesul • dezinfectează • ștergere • muta fișierele în carantină - Acțiune implicită pentru fișierele suspecte: • interzice accesul • ștergere • muta fișierele în carantină • nicio acțiune - Acțiune alternativă pentru fișierele suspecte: • interzice accesul • ștergere • mută fișierele în carantină. 2.3.2. Scanarea automată în timp real poate fi setată să nu scaneze arhive sau fișiere mai mari de « x » MB, mărimea fișierelor putând fi definită de administratorul soluției, 2.3.3. Scanarea automată a emailurilor la nivelul stației de lucru pentru POP3/SMTP. 2.3.4. Clientii antimalware pentru workstation să permită definirea unor liste de excludere de la scanarea în timp real și la cerere a anumitor directoare, discuri, fișiere, certificate, extensii sau procese, incluzând amprenta (hash) în cazul fișierelor sau certificatelor.	
--	--	--	---	--	--





“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

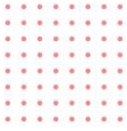
office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

			2.3.5. Posibilitatea de configura scanarile programate să se execute cu prioritate redusă. 2.3.6. Produsul antimalware poate fi configurat să foloseasca scanarea în cloud, și partial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalată în rețea. 2.3.7. Pentru o protecție sporită, soluția antimalware trebuie să aiba 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazată pe monitorizarea proceselor. 2.3.8. Pentru o mai buna gestionare a antimalware instalat pe stații, produsul trebuie să includă opțiunea de setare a unei parole pentru protecția la dezinstalare. 2.3.9. Pentru siguranta utilizatorului, clientul trebuie să includă un modul de antiphishing 2.3.10. Soluția trebuie să ofere o tehnologie de tip „preventiv / vaccin” ce va actiona împotriva potentialelor atacuri de tip ransomware. 2.3.11. Soluția trebuie să ofere un set de excluțiuni predefinite pentru Roluri de tip „server” Microsoft (DNS, DHCP, AD, Exchange, Sharepoint)	2.3.5. Posibilitatea de configura scanarile programate să se execute cu prioritate redusă. 2.3.6. Produsul antimalware poate fi configurat să foloseasca scanarea în cloud, și partial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o masina de scanare instalată în rețea. 2.3.7. Pentru o protecție sporită, soluția antimalware are 3 tipuri de detecție: bazată pe semnături, bazată de comportamentul fișierelor și bazată pe monitorizarea proceselor. 2.3.8. Pentru o mai buna gestionare a antimalware instalat pe stații, produsul include opțiunea de setare a unei parole pentru protecția la dezinstalare. 2.3.9. Pentru siguranta utilizatorului, clientul include un modul de antiphishing 2.3.10. Soluția oferă o tehnologie de tip „preventiv / vaccin” ce va actiona împotriva potentialelor atacuri de tip ransomware. 2.3.11. Soluția oferă un set de excluțiuni predefinite pentru Roluri de tip „server” Microsoft (DNS, DHCP, AD, Exchange, Sharepoint)	
--	--	--	--	--	--





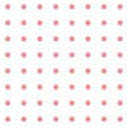
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			2.3.12. Soluția trebuie să poată detecta atacuri de tip „file-less” incluzând pe cele ce folosesc utilitare aferente sistemelor de operare de tip interpretor de script (powershell). 2.3.13. Soluția trebuie să ofere protecție în portivă atacurilor ransomware inițiate la distanță, de pe alte stații de lucru. 2.4 Anti-Exploit-Avansat: 2.4.1. Sa fie posibilitatea de a opri atacurile avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive. 2.4.2. Să depisteze în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 2.4.3. Sa fie protejate aplicațiile utilizate frecvent și a celor de tip „sistem” 2.5 Firewall: 2.5.1. Sa fie posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 2.5.2. Sa fie abilitatea de a detecta scanarea de porturi. 2.5.3. Sa fie posibilitatea de a seta diferite profiluri de rețea 2.5.4. Sa fie abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune 2.6 Carantina: 2.6.1. Produsul antimalware trebuia să permită stergerea automată a fișierelor carantinate mai	2.3.12. Soluția poate detecta atacuri de tip „file-less” incluzând pe cele ce folosesc utilitare aferente sistemelor de operare de tip interpretor de script (powershell). 2.3.13. Soluția oferă protecție în portivă atacurilor ransomware inițiate la distanță, de pe alte stații de lucru. 2.4 Anti-Exploit-Avansat: 2.4.1. Soluția permite oprirea atacurilor avansate de tip „zero-day” efectuate prin intermediul unor exploit-uri evazive. 2.4.2. Soluția depistează în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 2.4.3. Soluția protejează aplicațiile utilizate frecvent și a celor de tip „sistem” 2.5 Firewall: 2.5.1. Soluția oferă posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 2.5.2. Soluția este abilă de a detecta scanarea de porturi. 2.5.3. Soluția are posibilitatea de a seta diferite profiluri de rețea 2.5.4. Soluția permite crearea unor reguli personalizate bazate pe aplicație și/sau conexiune 2.6 Carantina: 2.6.1. Produsul antimalware permite stergerea automată a fișierelor carantinate mai	
--	--	--	--	---	--





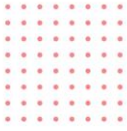
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare. 2.6.2. Posibilitatea de a restaura un fisier din carantina în locatia lui originala. 2.6.3. Modulul de carantina trebuia să permită salvarea unei copii a fisierului infectat respectiv transmiterea acestuia catre carantina înainte de a efectua orice alta acțiune asupra acestuia. 2.7 Protecția datelor: 2.7.1. Produsul trebuie să permită blocarea datelor confidentiale transmise prin HTTP sau SMTP prin crearea unor reguli specifice. 2.8 Controlul continutului: 2.8.1. Consola să detina integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati: • Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini. • Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii Prestabilite. 2.9 Controlul aplicatiilor: 2.9.1. Pentru o mai buna inventariere și administrare, soluția trebuie să includă o secțiune în consola de administrare unde se vor regăsi	vechi de o anumita perioada, pentru a nu incarca inutil spatiul de stocare. 2.6.2. Soluția are capacitatea de a restaura un fisier din carantina în locatia lui originala. 2.6.3. Modulul de carantina permite salvarea unei copii a fisierului infectat respectiv transmiterea acestuia catre carantina înainte de a efectua orice alta acțiune asupra acestuia. 2.7 Protecția datelor: 2.7.1. Produsul permite blocarea datelor confidentiale transmise prin HTTP sau SMTP prin crearea unor reguli specifice. 2.8 Controlul continutului: 2.8.1. Consola detine integrat un modul dedicat controlului accesului la Internet cu urmatoarele particularitati: • Permite blocarea accesului la Internet pentru anumite mașini client sau grupuri de mașini. • Permite restrictionarea accesului pe anumite pagini de internet dupa anumite categorii Prestabilite. 2.9 Controlul aplicatiilor: 2.9.1. Pentru o mai buna inventariere și administrare, soluția include o secțiune în consola de administrare unde se vor regăsi toate aplicatiile	
--	--	--	--	--	--





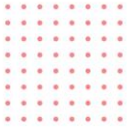
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			toate aplicatiile descoperite în rețea, grupate după: nume, versiune, descoperit la, găsit pe. 2.9.2. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subproces) după: • Cale fișier: local, CD-ROM, portabil sau rețea • Hash • Certificat 2.10 Controlul dispozitivelor: 2.10.1. Modulul să poată fi instalat/dezinstalat în funcție de preferința administratorului. 2.10.2. Modulul să permită controlul următoarelor tipuri de dispozitive: • Bluetooth Devices • CDROM Devices • Floppy Disk Drives • Security Policies 153 • IEEE 1284.4 • IEEE 1394 • Imaging Devices • Modems • Windows Portable • Printers • Network Adapters • Wireless Network Adapters • Internal and External Storage 2.10.3. Modulul să permită configurarea de reguli prin care se vor defini permisiunile pentru	descoperite în rețea, grupate după: nume, versiune, descoperit la, găsit pe. 2.9.2. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subproces) după: • Cale fișier: local, CD-ROM, portabil sau rețea • Hash • Certificat 2.10 Controlul dispozitivelor: 2.10.1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 2.10.2. Modulul permite controlul următoarelor tipuri de dispozitive: • Bluetooth Devices • CDROM Devices • Floppy Disk Drives • Security Policies 153 • IEEE 1284.4 • IEEE 1394 • Imaging Devices • Modems • Windows Portable • Printers • Network Adapters • Wireless Network Adapters • Internal and External Storage 2.10.3. Modulul permite configurarea de reguli prin care se vor defini permisiunile pentru	
--	--	--	--	---	--





“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

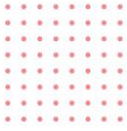
office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

			dispozitivele conectate la masina client cum ar fi: permis/blocat/custom respectiv să poată limita accesul dispozitivelor externe la „read only” sau limita doar accesul la porturile USB ale endpoint-ului permitând orice alt tip de dispozitiv ce nu foloseste acest tip de port/interfata. 2.11 Power User: 2.11.1. Modulul trebuie să poata fi instalat/dezinstalat în functie de preferinta administratorului. 2.12 Actualizare: 2.12.1. Soluția trebuie să permită efectuarea actualizarii la nivel de stație în mod silențios (fără avertizare). 2.12.2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). 2.12.3. Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are și rol de server de actualizare. 2.12.4. Abilitatea de a împiedica punctele finale să iasă pe internet pentru a descărca actualizări. 3. PROTECȚIE ȘI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE 3.1 Cerinte minime de sistem: 3.1.1. Exchange server 2019, 2016, 2013 cu rol de Edge Transport sau Mailbox	dispozitivele conectate la masina client cum ar fi: permis/blocat/custom respectiv să poată limita accesul dispozitivelor externe la „read only” sau limita doar accesul la porturile USB ale endpoint-ului permitând orice alt tip de dispozitiv ce nu foloseste acest tip de port/interfata. 2.11 Power User: 2.11.1. Modulul poate fi instalat/dezinstalat în functie de preferinta administratorului. 2.12 Actualizare: 2.12.1. Soluția permite efectuarea actualizarii la nivel de stație în mod silențios (fără avertizare). 2.12.2. Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). 2.12.3. Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are și rol de server de actualizare. 2.12.4. Soluția este abilă de a împiedica punctele finale să iasă pe internet pentru a descărca actualizări. 3. PROTECȚIE ȘI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE 3.1 Cerinte minime de sistem: 3.1.1. Exchange server 2019, 2016, 2013 cu rol de Edge Transport sau Mailbox	
--	--	--	--	--	--





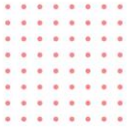
“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

			3.1.2. Microsoft Windows Server 2008R2 sau mai nou 3.1.3. Produsul să ofere protecție antimalware, antispam (inclusiv antiphishing), precum și filtrare de atasamente și conținut, prin integrarea cu serverul Microsoft Exchange. De asemenea, va permite scanarea antimalware la cerere a bazelor de date Exchange. 3.1.4. Produsul să asigure scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail. 3.1.5. Actualizarea antimalware trebuie să poată fi făcută automat la un interval de maxim 1 ora, precum și la cerere. 3.1.6. Produsul să ofere opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, stergere, mutare în carantina). 3.1.7. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va oferi protecție anti-spyware pentru a preveni furtul de date confidențiale. 3.1.8. Produsul să ofere protecție antispam, cu o bază de semnături actualizabilă prin internet.	3.1.2. Microsoft Windows Server 2008R2 sau mai nou 3.1.3. Produsul oferă protecție antimalware, antispam (inclusiv antiphishing), precum și filtrare de atasamente și conținut, prin integrarea cu serverul Microsoft Exchange. De asemenea, permite scanarea antimalware la cerere a bazelor de date Exchange. 3.1.4. Produsul asigură scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail. 3.1.5. Actualizarea antimalware poate fi făcută automat la un interval de maxim 1 ora, precum și la cerere. 3.1.6. Produsul oferă opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, stergere, mutare în carantina). 3.1.7. Cu ajutorul unei baze de date complete cu semnături de spyware și a euristicii de detecție a acestui tip de programe, produsul va oferi protecție anti-spyware pentru a preveni furtul de date confidențiale. 3.1.8. Produsul oferă protecție antispam, cu o bază de semnături actualizabilă prin internet.	
--	--	--	---	---	--





“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

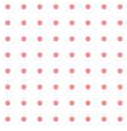
office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

			3.1.9. Modulul antispam trebuie să includă un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice. 3.1.10. Produsul trebuie să ofere filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje. 3.1.11. Produsul trebuie să ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou aparute. 3.1.12. Produsul să ofere posibilitatea de a defini politici de filtrare antimalware, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori. 3.1.13. Actualizarea produsului să fie configurabilă și să se putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu. 3.1.14. Produsul trebuie să ofere statistici atât referitoare la scanarea antivirus cât și la scanarea antispam. 3.1.15. Produsul să se integreze în cadrul consolei de management unitar al soluției antivirus. Pentru	3.1.9. Modulul antispam include un filtru URL cu o bază de adrese URL cunoscute a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice. 3.1.10. Produsul oferă filtru RBL care să identifice spam-ul prin sincronizarea cu anumite baze de date online care conțin liste de servere de mail cunoscute ca fiind la originea acestui tip de mesaje. 3.1.11. Produsul oferă un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou aparute. 3.1.12. Produsul oferă posibilitatea de a defini politici de filtrare antimalware, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori. 3.1.13. Actualizarea produsului să fie configurabilă și să se putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu. 3.1.14. Produsul oferă statistici atât referitoare la scanarea antivirus cât și la scanarea antispam. 3.1.15. Produsul se integrează în cadrul consolei de management unitar al soluției antivirus.	
--	--	--	--	--	--





“RTS ONE” S.R.L.
<https://rts.md>

(+373) 22 101 777
office@rts.one

str. Mitropolit
G. Bănulescu-Bodoni
59/B, of. 815

				usurința accesului la setările produsului din diferite medii de operare, produsul va avea consola de administrare web. 4. ALTE CERINȚE OBLIGATORII: • Pentru soluția oferată se solicită suport local și de la producător pentru 36 luni. • Producătorul trebuie să ofere suport 24/7, prin e-mail sau conectare de la distanță, inclusiv suport local. • Lucrările de instalare, configurare, punerea în funcțiune a soluției trebuie să fie executate de ofertant, iar costul acestora trebuie să fie incluse în oferta comercială. • Se va oferi manual de instalare și administrare a produsului oferat în limba română și engleză. • Prezentarea a minim 2 certificate tehnice a persoanelor certificate pe produsul oferat. • Ofertantul va prezenta Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul oferat. • Ofertantul va pune la dispoziție cel puțin o	Pentru usurița accesului la setările produsului din diferite medii de operare, produsul are consola de administrare web. 4. ALTE CERINȚE OBLIGATORII: • Soluția oferată include suport local și de la producător pentru 36 luni. • Atat producătorul cat si ofertantul oferă suport 24/7, prin e-mail sau conectare de la distanță. • Lucrările de instalare, configurare, punerea în funcțiune a soluției vor fi executate de ofertant, iar costul acestora este incluse în oferta comercială. • Se ofera manual de instalare și administrare a produsului oferat în limba română și engleză. • Prezentam 2 certificate tehnice a persoanelor certificate pe produsul Bitdefender. • Atasat la oferta prezentam Autorizarea de la producător care atestă dreptul de a livra bunuri/lucrări/servicii pe produsul oferat. • Vom pune la dispoziția Autorității Contractante o persoana certificata în calitate de auditor intern	
--	--	--	--	---	---	--





“RTS ONE” S.R.L.

<https://rts.md>

(+373) 22 101 777

office@rts.one

str. Mitropolit

G. Bănulescu-Bodoni
59/B, of. 815

				persoana certificata în calitate de auditor intern pentru sistemul de management al securității informațiilor conform ISO/IEC 27001:2018 în cazul apariției problemelor de securitate; • Termen de livrare: 15 zile lucrătoare de la data înregistrării contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.	pentru sistemul de management al securității informațiilor conform ISO/IEC 27001:2018 în cazul apariției problemelor de securitate; • Termen de livrare: 15 zile lucrătoare de la data înregistrării contractului, care include și timpul lucrărilor de instalare, configurare și punerea în funcțiune a soluției.	
TOTAL						

Semnat:

Ofertantul: „**RTS ONE**” S.R.L.

Numele, Prenumele: **CELONENCO Vitalie**

În calitate de: **Administrator**

Adresa: **mun.Chișinău, str.Mitropolit Gavriil Bănulescu-Bodoni, 59/B, of.815**

