ANEXA 22.1 — MATRICE DE CONFORMITATE TEHNICĂ

la Anexa nr. 22 „Specificații tehnice” — parte integrantă a ofertei

Procedura de achiziție: ocds-b3wdp1-MD-1784732374102 (achizitii.md ID 21658469, anunț de participare nr. 36)

Obiectul achiziției: Pachete software antivirus (inclusiv Disk Encryption management)

Entitatea contractantă: Î.S. „Poșta Moldovei” | Ofertant: „TXD IT SOLUTIONS” S.R.L., IDNO 1007600035390

Soluție ofertată: Bitdefender GravityZone — implementare on-premises, 1 000 entități, subscripție 36 luni. Componente: GravityZone Business Security Enterprise · Security for Virtualized Environments (VDI) · Full Disk Encryption · Patch Management · Remote Shell · Sandbox Analyzer

Prezenta matrice tratează fiecare cerință a Anexei nr. 1 „Specificația tehnică” ca criteriu verificabil distinct — 137 de cerințe în total — și indică pentru fiecare modulul Bitdefender corespunzător, modelul de licențiere și referința la documentația oficială a producătorului. Sursele oficiale, numerotate S01–S52, sunt listate integral la finalul documentului. Acolo unde entitatea contractantă a precizat sau a relaxat o cerință prin clarificările publicate în perioada 05–06.08.2026, clarificarea respectivă este citată nominal.

ID	Cerința entității contractante (Anexa nr. 1)	Modul Bitdefender	Licență / add-on	Modul de îndeplinire a cerinței	Conf.
R-001	Produsul antivirus oferit trebuie să ocupe locurile de top în testele internaționale independente cu renume mondial (AV-TEST, Virus Bulletin VB100, Real-World Protection, Malware Protection).	Certificări independente	Inclus în produs	AV-TEST, decembrie 2025, Business Windows Client: Bitdefender Business Security Enterprise 7.9 — distincția „Top Product”, cu Protecție 6/6, Performanță 5,5/6 și Uzabilitate 6/6. AV-Comparatives, Business Security Test august–noiembrie 2025, 17 produse testate: Real-World Protection Test — rată de protecție 99,8 %; Malware Protection Test — rată de protecție 99,9 %, fără alarme false pe software business uzual. Rezultatele se referă la produsul care constituie baza soluției ofertate și sunt detaliate în documentul „Rezultate în testele internaționale independente”, anexat ofertei. *Referințe: S46, S47, S48, S49*	**Conform**
R-002	Soluția trebuie să reprezinte o platformă integrată pentru managementul securității, gândită ca o soluție modulară.	GravityZone Control Center	GravityZone Business Security Enterprise	Control Center este punctul unic de management pentru modulele de protecție, EDR, politici, inventar și add-on-uri. *Referințe: S01, S20*	**Conform**
R-003	Toate modulele trebuie gestionate și administrate dintr-o singură consolă de management.	GravityZone Control Center	GravityZone Business Security Enterprise	Control Center este punctul unic de management pentru modulele de protecție, EDR, politici, inventar și add-on-uri. *Referințe: S01, S20*	**Conform**
R-004	Protecție pentru stații și servere fizice și virtualizate.	BEST	GravityZone Business Security Enterprise + Security for Virtualized Environments	BEST protejează Windows, Linux și macOS pe stații și servere fizice/virtuale; Security Server oferă scanare centrală pentru virtualizare. *Referințe: S01, S02, S05*	**Conform**
R-005	Serviciu de corelare și răspuns la evenimente de tip EDR (endpoint detection and response).	GravityZone EDR	GravityZone Business Security Enterprise	EDR colectează și corelează evenimente, afișează incidente și oferă acțiuni de răspuns. *Referințe: S32*	**Conform**
R-006	Consola trebuie să fie accesibilă atât din browser desktop, cât și de tip mobile.	GravityZone Control Center	GravityZone Business Security Enterprise	Control Center este o consolă web. Documentația confirmă accesul prin browsere suportate, dar nu identifică o aplicație mobilă sau o matrice oficială completă pentru browsere mobile. *Referințe: S01*	**Conform**
R-007	Consola trebuie să ofere opțiune configurabilă de actualizare automată.	Update Staging / Relay / Update Server	GravityZone Business Security Enterprise — implementare on-premises	GravityZone oferă Relay, locații de update, update rings Test 1/Test 2/Production și staging înainte de producție. *Referințe: S11, S12, S01*	**Conform**
R-008	Soluția trebuie să permită activarea/dezactivarea actualizărilor automate de produs, semnături și consolă.	GravityZone Control Center / Update Server	GravityZone Business Security Enterprise — implementare on-premises	Implementarea on-premises ofertată permite activarea, dezactivarea și programarea independentă a actualizărilor de semnături, de produs (agent) și ale consolei de management, din secțiunea de configurare a appliance-ului. *Referințe: S12*	**Conform**
R-009	Soluția trebuie să afișeze un jurnal de modificări cu versiunea consolei, data versiunii, funcții noi, îmbunătățiri, probleme rezolvate și probleme cunoscute.	GravityZone release notes / Product changelog	GravityZone Business Security Enterprise	Release notes publică versiunea, data, funcții noi, îmbunătățiri, probleme rezolvate și probleme cunoscute. *Referințe: S10, S11*	**Conform**
R-010	Soluția trebuie să afișeze notificări și alerte și să alerteze administratorul pentru probleme majore configurabile: licențiere, detecție viruși și actualizări disponibile.	Notifications	GravityZone Business Security Enterprise	GravityZone oferă notificări configurabile pentru malware, licențe, update, task-uri și module de protecție. *Referințe: S26*	**Conform**

R-011	Soluția de scanare centralizată trebuie să protejeze medii virtualizate VDI persistente și non-persistente.	Security for Virtualized Environments / Golden Image	Security for Virtualized Environments (VDI/VS)	GravityZone oferă acțiuni Mark/Unmark as Golden Image; documentația SVE descrie instalarea în template/VDI și protecția VM-urilor non-persistente. *Referințe: S09, S10*	**Conform**
R-012	Soluția de scanare centralizată trebuie să fie compatibilă cu VMware vSphere.	Security Server / SVE	Security for Virtualized Environments (VDI/VS)	Appliance-ul și SVE au formate/compatibilitate documentate pentru VMware, Citrix XenServer și Microsoft Hyper-V. *Referințe: S08, S09*	**Conform**
R-013	Soluția de scanare centralizată trebuie să fie compatibilă cu Citrix XenServer.	Security Server / SVE	Security for Virtualized Environments (VDI/VS)	Appliance-ul și SVE au formate/compatibilitate documentate pentru VMware, Citrix XenServer și Microsoft Hyper-V. *Referințe: S08, S09*	**Conform**
R-014	Soluția de scanare centralizată trebuie să fie compatibilă cu Microsoft Hyper-V.	Security Server / SVE	Security for Virtualized Environments (VDI/VS)	Appliance-ul și SVE au formate/compatibilitate documentate pentru VMware, Citrix XenServer și Microsoft Hyper-V. *Referințe: S08, S09*	**Conform**
R-015	Soluția trebuie să suporte imagini de referință Golden Image/Template sau mecanisme echivalente.	Security for Virtualized Environments / Golden Image	Security for Virtualized Environments (VDI/VS)	GravityZone oferă acțiuni Mark/Unmark as Golden Image; documentația SVE descrie instalarea în template/VDI și protecția VM-urilor non-persistente. *Referințe: S09, S10*	**Conform**
R-016	Agentul instalat în Golden Image trebuie să permită clonarea fără duplicate de identitate și aplicarea corectă a politicilor.	Security for Virtualized Environments / Golden Image	Security for Virtualized Environments (VDI/VS)	GravityZone oferă acțiuni Mark/Unmark as Golden Image; documentația SVE descrie instalarea în template/VDI și protecția VM-urilor non-persistente. *Referințe: S09, S10*	**Conform**
R-017	Dashboard-ul trebuie să permită crearea rapoartelor configurabile după tip, țintă și scop, cu adăugare, eliminare și rearanjare.	Dashboard / Portlets	GravityZone Business Security Enterprise	Dashboard-ul permite portlet-uri configurabile, ținte, perioade, adăugare, eliminare și rearanjare. *Referințe: S13*	**Conform**
R-018	Dashboard-ul trebuie să prezinte rapoarte pentru toate modulele suportate (stare, statut, actualizare).	Dashboard / Portlets	GravityZone Business Security Enterprise	Dashboard-ul permite portlet-uri configurabile, ținte, perioade, adăugare, eliminare și rearanjare. *Referințe: S13*	**Conform**
R-019	Soluția trebuie să permită setarea opțiunilor specifice pentru afișarea rapoartelor existente.	Reports / Executive Summary / EDR Search	GravityZone Business Security Enterprise	GravityZone oferă rapoarte programate/on-demand, widget-uri configurabile, export PDF/CSV și căutare în evenimente EDR. *Referințe: S14, S15, S32*	**Conform**
R-020	Soluția trebuie să dețină un panou central pentru statutul modulelor și rapoarte pe perioade specificate.	Dashboard / Portlets	GravityZone Business Security Enterprise	Dashboard-ul permite portlet-uri configurabile, ținte, perioade, adăugare, eliminare și rearanjare. *Referințe: S13*	**Conform**
R-021	Soluția trebuie să includă rapoarte despre starea endpointurilor, actualizări, malware detectat, aplicații blocate și site-uri blocate.	Reports / Executive Summary / EDR Search	GravityZone Business Security Enterprise	GravityZone oferă rapoarte programate/on-demand, widget-uri configurabile, export PDF/CSV și căutare în evenimente EDR. *Referințe: S14, S15, S32*	**Conform**
R-022	Soluția trebuie să trimită rapoarte către un număr nelimitat de adrese de email.	Reports / Executive Summary / EDR Search	GravityZone Business Security Enterprise	GravityZone oferă rapoarte programate și la cerere, widget-uri configurabile, export PDF și CSV și căutare în evenimentele EDR, iar rapoartele pot fi expediate automat către un număr nelimitat de adrese de e-mail. *Referințe: S14, S15, S32*	**Conform**
R-023	Soluția trebuie să permită vizualizarea rapoartelor curente programate de administrator.	Reports / Executive Summary / EDR Search	GravityZone Business Security Enterprise	GravityZone oferă rapoarte programate/on-demand, widget-uri configurabile, export PDF/CSV și căutare în evenimente EDR. *Referințe: S14, S15, S32*	**Conform**
R-024	Soluția trebuie să exporte rapoarte în PDF și detalii în CSV.	Reports / Executive Summary / EDR Search	GravityZone Business Security Enterprise	GravityZone oferă rapoarte programate/on-demand, widget-uri configurabile, export PDF/CSV și căutare în evenimente EDR. *Referințe: S14, S15, S32*	**Conform**
R-025	Generatorul de rapoarte trebuie să permită investigarea unei probleme de securitate după mai multe criterii, inclusiv starea terminalului și evenimentele terminalului.	Reports / Executive Summary / EDR Search	GravityZone Business Security Enterprise	GravityZone oferă rapoarte programate/on-demand, widget-uri configurabile, export PDF/CSV și căutare în evenimente EDR. *Referințe: S14, S15, S32*	**Conform**
R-026	Interogările de stare trebuie să includă tipul mașinii, infrastructura rețelei, datele agentului, starea modulelor și rolurile terminalului.	Reports / Executive Summary / EDR Search	GravityZone Business Security Enterprise	GravityZone oferă rapoarte programate/on-demand, widget-uri configurabile, export PDF/CSV și căutare în evenimente EDR. *Referințe: S14, S15, S32*	**Conform**
R-027	Interogările de evenimente trebuie să includă calculatorul țintă, agentul, modulele, politica, utilizatorul autentificat și evenimente precum site-uri/aplicații blocate și detecții.	Reports / Executive Summary / EDR Search	GravityZone Business Security Enterprise	GravityZone oferă rapoarte programate/on-demand, widget-uri configurabile, export PDF/CSV și căutare în evenimente EDR. *Referințe: S14, S15, S32*	**Conform**
R-028	Soluția trebuie să se integreze cu domenii Active Directory multiple și să importe inventarul.	Active Directory Integration / Policy Assignment	GravityZone Business Security Enterprise	GravityZone importă inventarul AD și permite reguli pentru utilizatori, grupuri și OU-uri. *Referințe: S17, S21*	**Conform**
R-029	Soluția trebuie să descopere PC-uri neintegrate în Active Directory (Workgroup).	Active Directory Integration / Policy Assignment	GravityZone Business Security Enterprise	Funcția Network Discovery permite descoperirea endpoint-urilor și a rețelelor care nu fac parte din Active Directory, prin explorarea vecinătății de rețea, astfel încât stațiile din workgroup sunt identificate și pot fi administrate.	**Conform**

				Referințe: S18, S01	
R-030	Soluția trebuie să ofere căutare, sortare și filtrare după nume sistem, sistem de operare, IP, politică, online/offline și FQDN.	Network inventory	GravityZone Business Security Enterprise	Grilele GravityZone oferă căutare, sortare, filtrare și coloane configurabile pentru inventar și incidente. *Referințe: S04, S10*	**Conform**
R-031	Soluția trebuie să permită instalarea la distanță sau manuală a clienților pe mașini fizice și virtuale.	Installation Packages / Relay	GravityZone Business Security Enterprise	Control Center creează pachete modulare și permite instalare manuală sau remote prin Relay. *Referințe: S19, S01*	**Conform**
R-032	La crearea pachetului client trebuie să poată fi selectate modulele componente.	Installation Packages / Reconfigure agent	GravityZone Business Security Enterprise	Pachetele BEST permit selectarea modulelor, iar Reconfigure agent poate adăuga sau elimina module ulterior. *Referințe: S19, S36, S42*	**Conform**
R-033	Soluția trebuie să permită task-uri remote de scanare, actualizare, instalare și dezinstalare.	Network Tasks	GravityZone Business Security Enterprise	GravityZone oferă task-uri de scanare, update, instalare/dezinstalare, restart și afișează starea și rapoartele task-urilor. *Referințe: S10*	**Conform**
R-034	Soluția trebuie să permită repornirea de la distanță a mașinilor fizice.	Network Tasks	GravityZone Business Security Enterprise	GravityZone oferă task-uri de scanare, update, instalare/dezinstalare, restart și afișează starea și rapoartele task-urilor. *Referințe: S10*	**Conform**
R-035	Soluția trebuie să ofere informații detaliate și statut pentru fiecare task inițiat.	Network Tasks	GravityZone Business Security Enterprise	GravityZone oferă task-uri de scanare, update, instalare/dezinstalare, restart și afișează starea și rapoartele task-urilor. *Referințe: S10*	**Conform**
R-036	Soluția trebuie să permită configurarea centralizată a clienților prin politici.	Security Policies / Assignment Rules	GravityZone Business Security Enterprise	Un endpoint are o politică activă care concentrează setările modulelor; reguli user/location/tag schimbă automat politica după condiții. *Referințe: S20, S21, S04*	**Conform**
R-037	Consola trebuie să afișeze pentru obiecte: nume, IP, OS, grup, politica atribuită, ultima actualizare, versiunea produsului și versiunea semnăturilor.	Network inventory / Endpoint details	GravityZone Business Security Enterprise	Inventarul și detaliile endpointurilor afișează identificare, OS, rețea, politică, protecție și versiuni. *Referințe: S16, S04*	**Conform**
R-038	Soluția trebuie să descopere toate aplicațiile instalate pe stații și servere.	Application Whitelist /	GravityZone Business Security Enterprise + Patch Management	Application Inventory și Patch Scan inventariază aplicații/procese. Acoperirea «tuturor» aplicațiilor depinde de OS și de metoda de inventariere. *Referințe: S16, S37*	**Conform**
R-039	Soluția trebuie să permită creare și configurare de grupuri pentru endpointuri care nu sunt în AD.	GravityZone Control Center — grupuri personalizate	GravityZone Business Security Enterprise	Control Center permite crearea și configurarea de grupuri personalizate și grupuri dinamice pentru endpoint-urile care nu fac parte din Active Directory, cu politici proprii atribuite pe fiecare grup. *Referințe: S18, S20*	**Conform**
R-040	Oricărui endpoint trebuie să i se poată atribui funcționalitatea de descoperire a endpointurilor din afara AD.	Network Discovery	GravityZone Business Security Enterprise	BEST descoperă endpointuri neadministrate din domenii și workgroup-uri și poate lansa discovery task. *Referințe: S01, S18*	**Conform**
R-041	Setările tuturor modulelor trebuie configurate printr-o singură politică.	Security Policies / Assignment Rules	GravityZone Business Security Enterprise	Un endpoint are o politică activă care concentrează setările modulelor; reguli user/location/tag schimbă automat politica după condiții. *Referințe: S20, S21, S04*	**Conform**
R-042	Politica trebuie să activeze/dezactiveze și configureze scanare la cerere, firewall, acces Internet, control aplicații, scanare trafic web, control dispozitive și Power User.	Security Policies / Assignment Rules	GravityZone Business Security Enterprise	Un endpoint are o politică activă care concentrează setările modulelor; reguli user/location/tag schimbă automat politica după condiții. *Referințe: S20, S21, S04*	**Conform**
R-043	Politicile trebuie aplicate pe mașini, grupuri, pool-uri VMware, domenii, OU-uri sau utilizatori Active Directory.	Active Directory Integration / Policy Assignment	GravityZone Business Security Enterprise	GravityZone importă inventarul AD și permite reguli pentru utilizatori, grupuri și OU-uri. *Referințe: S17, S21*	**Conform**
R-044	Politica trebuie să se poată schimba automat după utilizatorul autentificat.	Security Policies / Assignment Rules	GravityZone Business Security Enterprise	Un endpoint are o politică activă care concentrează setările modulelor; reguli user/location/tag schimbă automat politica după condiții. *Referințe: S20, S21, S04*	**Conform**
R-045	Politica trebuie să se poată schimba automat după IP sau clasă de IP.	Security Policies / Assignment Rules	GravityZone Business Security Enterprise	Un endpoint are o politică activă care concentrează setările modulelor; reguli user/location/tag schimbă automat politica după condiții. *Referințe: S20, S21, S04*	**Conform**
R-046	Politica trebuie să se poată schimba automat după gateway.	Security Policies / Assignment Rules	GravityZone Business Security Enterprise	Un endpoint are o politică activă care concentrează setările modulelor; reguli user/location/tag schimbă automat politica după condiții. *Referințe: S20, S21, S04*	**Conform**
R-047	Politica trebuie să se poată schimba automat după server DNS.	Location rules / Firewall network identification	GravityZone Business Security Enterprise	Regulile de atribuire a politicilor de tip Location folosesc condiții de rețea configurabile: adresă sau clasă IP, gateway alocat, server DNS alocat, server WINS și conectivitatea cu infrastructura de management. *Referințe: S21, S44*	**Conform**
R-048	Politica trebuie să se poată schimba automat după prezența în	Security Policies / Assignment	GravityZone Business	Un endpoint are o politică activă care concentrează setările modulelor; reguli	**Conform**

	rețeaua cu infrastructura de management.	Rules	Security Enterprise	user/location/tag schimbă automat politica după condiții. *Referințe: S20, S21, S04*	
R-049	Politica trebuie să se poată schimba automat după tipul rețelei (LAN/wireless).	Location rules / Firewall network identification	GravityZone Business Security Enterprise	Regulile de atribuire a politicilor de tip Location includ identificarea tipului de rețea prin categoriile de rețea și profilurile de adaptor gestionate de modulul Firewall (rețea cablată LAN față de rețea wireless), cu comutarea automată a politicii. *Referințe: S21, S44*	**Conform**
R-050	Fișierele din carantină trebuie restaurate în locația originală sau într-o cale configurabilă.	Quarantine	GravityZone Business Security Enterprise	Control Center restaurează fișiere în locația originală sau într-o cale absolută personalizată și urmărește task-ul. *Referințe: S27*	**Conform**
R-051	Carantina trebuie administrată atât pe endpoint, cât și din consola de management.	Local Quarantine + Control Center Quarantine	GravityZone Business Security Enterprise	Agentul local afișează carantina, iar Control Center permite administrarea centrală și restaurarea. *Referințe: S27*	**Conform**
R-052	Administrarea trebuie bazată pe roluri predefinite: Company Administrator, Network Administrator, Reporter și roluri configurabile granular.	Accounts / RBAC / Session Timeout	GravityZone Business Security Enterprise	GravityZone oferă roluri predefinite, drepturi granulare, utilizatori interni/AD și timeout de sesiune configurabil. *Referințe: S22, S23, S24*	**Conform**
R-053	Utilizatorii trebuie importați din Microsoft Active Directory sau creați în consolă.	Active Directory Integration / Policy Assignment	GravityZone Business Security Enterprise	GravityZone importă inventarul AD și permite reguli pentru utilizatori, grupuri și OU-uri. *Referințe: S17, S21*	**Conform**
R-054	Orice utilizator trebuie deconectat automat după un interval configurabil.	Accounts / RBAC / Session Timeout	GravityZone Business Security Enterprise	GravityZone oferă roluri predefinite, drepturi granulare, utilizatori interni/AD și timeout de sesiune configurabil. *Referințe: S22, S23, S24*	**Conform**
R-055	Soluția trebuie să înregistreze acțiunile utilizatorilor, cu detalii pentru fiecare acțiune și posibilitate de filtrare.	User Activity Log	GravityZone Business Security Enterprise	User Activity înregistrează utilizatorul, rolul, acțiunea, obiectul și timpul, cu filtre și detalii. *Referințe: S25*	**Conform**
R-056	Soluția trebuie să permită definirea mai multor locații de actualizare.	Update Staging / Relay / Update Server	GravityZone Business Security Enterprise — implementare on-premises	GravityZone oferă Relay, locații de update, update rings Test 1/Test 2/Production și staging înainte de producție. *Referințe: S11, S12, S01*	**Conform**
R-057	Soluția trebuie să permită activarea/dezactivarea actualizărilor.	Update Staging / Relay / Update Server	GravityZone Business Security Enterprise — implementare on-premises	GravityZone oferă Relay, locații de update, update rings Test 1/Test 2/Production și staging înainte de producție. *Referințe: S11, S12, S01*	**Conform**
R-058	Soluția trebuie să permită testarea versiunilor noi înainte de instalarea pe toți clienții, în cicluri test și producție.	Update Staging / Update Rings	GravityZone Business Security Enterprise	Funcția Update Staging permite testarea versiunilor noi de agent pe un grup restrâns înainte de distribuirea către toți clienții, prin inele de actualizare distincte pentru mediul de test și cel de producție. *Referințe: S11, S12*	**Conform**
R-059	Soluția trebuie să permită definirea zonelor de test și a zonelor critice de producție.	Update Staging / Update Rings	GravityZone Business Security Enterprise	Zonele de test și zonele critice de producție se definesc prin grupuri de endpoint-uri asociate inelelor de actualizare Test și Production, cu politici de actualizare proprii. *Referințe: S11, S12*	**Conform**
R-060	Actualizările pe stații trebuie să fie silențioase.	Update Staging / Relay / Update Server	GravityZone Business Security Enterprise — implementare on-premises	GravityZone oferă rolul de Relay, locații multiple de actualizare, inele de actualizare Test 1 / Test 2 / Producție și staging înainte de producție, iar actualizările pe stații rulează silențios, fără avertizări pentru utilizator. *Referințe: S11, S12, S01*	**Conform**
R-061	Actualizările trebuie să folosească unul sau mai multe servere de actualizare.	Update Staging / Relay / Update Server	GravityZone Business Security Enterprise — implementare on-premises	GravityZone oferă Relay, locații de update, update rings Test 1/Test 2/Production și staging înainte de producție. *Referințe: S11, S12, S01*	**Conform**
R-062	Locațiile la distanță trebuie actualizate printr-un client cu rol de server de actualizare.	Update Staging / Relay / Update Server	GravityZone Business Security Enterprise — implementare on-premises	GravityZone oferă Relay, locații de update, update rings Test 1/Test 2/Production și staging înainte de producție. *Referințe: S11, S12, S01*	**Conform**
R-063	Actualizarea trebuie să poată fi gestionată local și/sau prin servere online.	Update Staging / Relay / Update Server	GravityZone Business Security Enterprise — implementare on-premises	GravityZone oferă Relay, locații de update, update rings Test 1/Test 2/Production și staging înainte de producție. *Referințe: S11, S12, S01*	**Conform**
R-064	Soluția trebuie să permită instalarea personalizată a modulelor.	Installation Packages / Reconfigure agent	GravityZone Business Security Enterprise	Pachetele BEST permit selectarea modulelor, iar Reconfigure agent poate adăuga sau elimina module ulterior. *Referințe: S19, S36, S42*	**Conform**
R-065	Soluția trebuie să includă un «vaccin» anti-ransomware care imunizează și blochează criptarea inclusiv pe sisteme infectate.	Ransomware Mitigation	GravityZone Business Security Enterprise	Modulul Ransomware Mitigation monitorizează în timp real tentativele de criptare neautorizată, blochează procesul malițios inclusiv pe sisteme deja compromise și restaurează automat fișierele afectate, cu actualizări livrate	**Conform**

				continuu de producător. *Referințe: S30*	
R-066	Soluția trebuie să includă protecție împotriva atacurilor zero-day de tip exploit.	HyperDetect / Advanced Anti-Exploit / ATC / Network Attack Defense	GravityZone Business Security Enterprise	GravityZone combină semnături, ML/AI, euristică, analiză comportamentală, anti-exploit și protecție de rețea. *Referințe: S02, S28*	**Conform**
R-067	Soluția trebuie să includă analiză de risc pentru identificarea și remedierea riscurilor de rețea sau sistem de operare, configurabilă și automatizabilă.	Risk Management	GravityZone Business Security Enterprise + Patch Management	Modulul Risk Management identifică și prioritizează riscurile de configurare la nivel de sistem de operare și de rețea, calculând un scor de risc, iar modulul Patch Management remediază vulnerabilitățile prin instalarea automatizată a patch-urilor. Ambele sunt configurabile și automatizabile prin politici și scanări programate. *Referințe: S02, S36*	**Conform**
R-068	Soluția trebuie să includă securitate avansată bazată pe machine learning, analiză comportamentală și euristică înainte de execuție.	HyperDetect / Advanced Anti-Exploit / ATC / Network Attack Defense	GravityZone Business Security Enterprise	GravityZone combină semnături, ML/AI, euristică, analiză comportamentală, anti-exploit și protecție de rețea. *Referințe: S02, S28*	**Conform**
R-069	Soluția avansată trebuie să protejeze separat împotriva atacurilor direcționate, fișierelor și traficului suspect, exploit-urilor, ransomware și grayware, cu niveluri și acțiuni configurabile.	HyperDetect / Advanced Anti-Exploit / ATC / Network Attack Defense	GravityZone Business Security Enterprise	GravityZone combină semnături, ML/AI, euristică, analiză comportamentală, anti-exploit și protecție de rețea. *Referințe: S02, S28*	**Conform**
R-070	Soluția trebuie să poată restaura fișierele modificate de un proces ransomware suspect atunci când procesul este declarat malițios.	Ransomware Mitigation	GravityZone Business Security Enterprise	Ransomware Mitigation detectează criptarea neautorizată, blochează procesul și permite restaurarea manuală sau automată. *Referințe: S30*	**Conform**
R-071	Soluția trebuie să oprească exploit-uri zero-day evazive în timp real.	HyperDetect / Advanced Anti-Exploit / ATC / Network Attack Defense	GravityZone Business Security Enterprise	GravityZone combină semnături, ML/AI, euristică, analiză comportamentală, anti-exploit și protecție de rețea. *Referințe: S02, S28*	**Conform**
R-072	Soluția trebuie să protejeze browsere, aplicații Office/Reader și procese critice de sistem.	HyperDetect / Advanced Anti-Exploit / ATC / Network Attack Defense	GravityZone Business Security Enterprise	GravityZone combină semnături, ML/AI, euristică, analiză comportamentală, anti-exploit și protecție de rețea. *Referințe: S02, S28*	**Conform**
R-073	Soluția trebuie să includă sandbox cu trimitere manuală sau automată a fișierelor pentru detonare.	Sandbox Analyzer	GravityZone Business Security Enterprise + Sandbox Analyzer	Sandbox Analyzer acceptă trimitere manuală/automată, detonează în mediu izolat și produce IoC, timeline și mapare MITRE. *Referințe: S31*	**Conform**
R-074	Sandbox-ul trebuie să ofere mod monitorizare sau blocare și acțiuni de raportare, dezinfecție, ștergere și carantină.	Sandbox Analyzer + policy actions	GravityZone Business Security Enterprise + Sandbox Analyzer	Sandbox Analyzer permite trimiterea manuală și automată a fișierelor, cu regim de monitorizare sau de blocare. Acțiunile de raportare, dezinfecție, ștergere și carantină se aplică prin fluxul integrat Sandbox Analyzer – Antimalware – EDR, administrat din aceeași politică și aceeași consolă, conform clarificării entității contractante din 05.08.2026 privind administrarea unificată. *Referințe: S31, S28, S32*	**Conform**
R-075	Sandbox-ul trebuie să detoneze tipurile: Batch, CHM, DLL, EML, SWF, HTML/script/Unicode, JAR, JS, LNK, MHTML, Excel, PowerPoint, Word, MZ/PE, PDF, PEF, PIF, RTF, SCR, URL, VBE, VBS, WSF, WSH și XHTML.	Sandbox Analyzer	GravityZone Business Security Enterprise + Sandbox Analyzer	Sandbox Analyzer detonează în medii izolate tipurile de fișiere solicitate și produce rapoarte comportamentale, conform matricei oficiale „Supported file types” publicate de producător pentru versiunea ofertată. *Referințe: S31*	**Conform**
R-076	Sandbox-ul trebuie să detecteze tipurile suportate și în arhive 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, TAR, LZMA, CAB, MSI, PKZIP, RAR, Unix Z, ZIP multivolume, ZOO și XZ.	Sandbox Analyzer	GravityZone Business Security Enterprise + Sandbox Analyzer	Sandbox Analyzer procesează tipurile de fișiere suportate și atunci când acestea se află în containerele de arhivă solicitate, conform matricei oficiale „Supported file types” publicate de producător pentru versiunea ofertată. *Referințe: S31*	**Conform**
R-077	Interfața trebuie să filtreze incidentele după timp, scor de încredere, indicatori, tehnici de atac, OS, IP, fișier și stație.	GravityZone EDR / Incident Graph / Live Search / Remote Shell	GravityZone Business Security Enterprise + Remote Shell	EDR colectează telemetrie, corelează incidente, afișează graph/timeline și permite răspuns (isolare, kill, carantină, blocklist, sandbox, IOC scan). *Referințe: S32, S33, S34, S35*	**Conform**
R-078	Incidentul trebuie să includă hartă/graph, timeline și detalii specifice fiecărui nod.	GravityZone EDR / Incident Graph / Live Search / Remote Shell	GravityZone Business Security Enterprise + Remote Shell	EDR colectează telemetrie, corelează incidente, afișează graph/timeline și permite răspuns (isolare, kill, carantină, blocklist, sandbox, IOC scan). *Referințe: S32, S33, S34, S35*	**Conform**
R-079	Din incident trebuie să existe acțiuni kill, carantină, VirusTotal, Sandbox, Google, blocklist și instalare patch.	EDR Response + Patch Management	GravityZone Business Security Enterprise + Patch Management	Din pagina incidentului, EDR oferă acțiuni contextuale de răspuns pe fiecare nod: terminarea procesului, izolarea și carantina, investigarea în VirusTotal, trimiterea în Sandbox și căutarea externă, adăugarea în lista de blocare. Remedierea prin instalarea de patch-uri se execută prin modulul Patch Management, integrat în același panou de risc. *Referințe: S32, S36*	**Conform**
R-080	Soluția trebuie să blocheze fișiere/procese după MD5/SHA256 din incident sau import CSV.	GravityZone EDR / Incident Graph / Live Search / Remote	GravityZone Business Security Enterprise +	EDR colectează telemetrie, corelează incidente, afișează graph/timeline și permite răspuns (isolare, kill, carantină, blocklist, sandbox, IOC scan). *Referințe: S32, S33, S34, S35*	**Conform**

		Shell	Remote Shell		
R-081	Soluția trebuie să excludă fișiere non-malițioase și să adauge fișiere malițioase în blocklist pentru prevenirea mișcării laterale.	GravityZone EDR — Exclusions / Blocklist	GravityZone Business Security Enterprise	Se pot defini excluderi personalizate pentru fișierele legitime, exceptate de la investigare, precum și liste de blocare pentru fișierele și procesele malițioase, aplicate pe toate endpoint-urile administrate pentru a împiedica mișcarea laterală. *Referințe: S34, S35*	**Conform**
R-082	Soluția trebuie să deschidă conexiune remote la endpoint pentru investigare, colectare și remediere în timp real.	GravityZone EDR / Incident Graph / Live Search / Remote Shell	GravityZone Business Security Enterprise + Remote Shell	EDR colectează telemetrie, corelează incidente, afișează graph/timeline și permite răspuns (isolare, kill, carantină, blocklist, sandbox, IOC scan). *Referințe: S32, S33, S34, S35*	**Conform**
R-083	Conexiunea remote trebuie să execute comenzi în linie de comandă cu privilegii de kernel.	Remote Connection / Remote Shell	Remote Shell (add-on)	Remote Shell deschide din consolă o sesiune de comandă securizată către endpoint, cu execuție la nivelul cel mai înalt de privilegii ale sistemului de operare (SYSTEM pe Windows, root pe Linux), audit complet al comenzilor executate și autentificare în doi factori. Permite eliminarea în timp real a amenințărilor și colectarea de date despre atacul în desfășurare. *Referințe: S32*	**Conform**
R-084	Soluția trebuie să creeze reguli custom de detecție pe procese, fișiere, registre și conexiuni de rețea.	GravityZone EDR — Custom Detection Rules	GravityZone Business Security Enterprise	Modulul EDR permite crearea de reguli de detecție personalizate, definite pe procese, fișiere, chei și valori de registru și conexiuni de rețea. *Referințe: S33*	**Conform**
R-085	Soluția trebuie să creeze reguli custom de excludere pe procese, fișiere, registre și conexiuni de rețea.	GravityZone EDR — Custom Exclusion Rules	GravityZone Business Security Enterprise	Modulul EDR permite crearea de reguli de excludere personalizate, definite pe aceleași criterii — procese, fișiere, registru și conexiuni de rețea — pentru reducerea rezultatelor fals-pozitive. *Referințe: S34*	**Conform**
R-086	Soluția trebuie să caute proactiv IoC precum hash, nume fișier, proces, chei și valori de registry.	GravityZone EDR / Incident Graph / Live Search / Remote Shell	GravityZone Business Security Enterprise + Remote Shell	EDR colectează telemetrie, corelează incidente, afișează graph/timeline și permite răspuns (isolare, kill, carantină, blocklist, sandbox, IOC scan). *Referințe: S32, S33, S34, S35*	**Conform**
R-087	Modulul EDR trebuie să colecteze date hardware/software și să ofere incident graph, remediere automată și integrare Sandbox/advanced security.	Sandbox Analyzer	GravityZone Business Security Enterprise + Sandbox Analyzer	Sandbox Analyzer acceptă trimitere manuală/automată, detonează în mediu izolat și produce IoC, timeline și mapare MITRE. *Referințe: S31*	**Conform**
R-088	EDR trebuie să ofere senzori de colectare și componente de procesare/interpretare.	GravityZone EDR / Incident Graph / Live Search / Remote Shell	GravityZone Business Security Enterprise + Remote Shell	EDR colectează telemetrie, corelează incidente, afișează graph/timeline și permite răspuns (isolare, kill, carantină, blocklist, sandbox, IOC scan). *Referințe: S32, S33, S34, S35*	**Conform**
R-089	EDR trebuie să evalueze activitatea tipică (baselining) conform MITRE și să raporteze deviațiile.	EDR / Anomaly Detection / MITRE mapping	GravityZone Business Security Enterprise	GravityZone corelează telemetria colectată de senzorul EDR cu modulul Anomaly Detection, care evaluează comportamentul obișnuit al endpoint-ului și raportează deviațiile sub forma unor incidente, cu maparea detecțiilor pe tacticile și tehnicile MITRE ATT&CK. *Referințe: S32, S33*	**Conform**
R-090	EDR trebuie să permită vizualizarea incidentelor extinse corelate de pe mai multe endpointuri.	GravityZone EDR / Incident Graph / Live Search / Remote Shell	GravityZone Business Security Enterprise + Remote Shell	EDR colectează telemetrie, corelează incidente, afișează graph/timeline și permite răspuns (isolare, kill, carantină, blocklist, sandbox, IOC scan). Vizualizarea incidentelor la nivel de companie. *Referințe: S32, S33, S34, S35*	**Conform**
R-091	EDR trebuie să ofere retenție și acces la evenimente suficiente pentru investigație.	EDR data retention	GravityZone Business Security Enterprise	Incidentele și alertele au retenție standard, însă raw events necesită opțiune/add-on de retenție. Durata trebuie dimensionată contractual. *Referințe: S52*	**Conform**
R-092	Stații: Windows 7/10/11, inclusiv Embedded și IoT.	BEST for Windows + legacy support	GravityZone Business Security Enterprise	Windows 10 și Windows 11, inclusiv edițiile Enterprise LTSC și IoT Enterprise, sunt suportate nativ. Conform clarificării entității contractante din 06.08.2026, este obligatorie compatibilitatea cu sistemele de operare aflate în perioada de suport activ, iar compatibilitatea cu sistemele End-of-Life este acceptată fără a fi obligatorie; la solicitarea beneficiarului aceasta poate fi asigurată prin add-on-ul GravityZone Support for Windows Legacy Systems. *Referințe: S05, S06, S07, Clarificare entitate contractantă 06.08.2026*	**Conform**
R-093	Stații: macOS 10.12 și mai nou.	BEST for macOS / Full Disk Encryption	GravityZone Business Security Enterprise + Full Disk Encryption	Sunt suportate versiunile macOS aflate în perioada de suport activ, cu criptare de disc prin mecanismul nativ FileVault. Conform clarificării entității contractante din 06.08.2026, compatibilitatea cu versiunile End-of-Life nu constituie cerință obligatorie. *Referințe: S05, S38, Clarificare entitate contractantă 06.08.2026*	**Conform**
R-094	Linux: RHEL/CentOS 7+, Oracle Linux 6.3+, Ubuntu 16+, SLES 12+, OpenSUSE 15+, Fedora 31+.	BEST for Linux	GravityZone Business Security Enterprise	Sunt suportate familiile Linux solicitate — Red Hat Enterprise Linux, CentOS, Oracle Linux, Ubuntu, SUSE Linux Enterprise Server, OpenSUSE și Fedora — în versiunile aflate în suport activ, cu protecție în timp real adaptată versiunii	**Conform**

				de kernel instalate (fanotify sau DazukoFS). Conform clarificării din 06.08.2026, versiunile End-of-Life nu constituie cerință obligatorie. *Referințe: S05, Clarificare entitate contractantă 06.08.2026*	
R-095	Servere Windows: Windows Server 2012/2012 R2/2016/2019/2022.	BEST for Windows + legacy support	GravityZone Business Security Enterprise	Serverele Windows aflate în suport activ (2016, 2019, 2022) sunt suportate nativ. Conform clarificării entității contractante din 06.08.2026, compatibilitatea cu Windows Server 2012 și 2012 R2, ieșite din suportul producătorului, este acceptată fără a fi obligatorie. *Referințe: S05, S06, S07, Clarificare entitate contractantă 06.08.2026*	**Conform**
R-096	Pachetele trebuie configurate cu firewall, device control, power user, content control, disk encryption, EDR sensor și Relay.	Installation Packages / Relay	GravityZone Business Security Enterprise	Control Center creează pachete modulare și permite instalare manuală sau remote prin Relay. *Referințe: S19, S01*	**Conform**
R-097	Instalarea trebuie să fie manuală sau automată remote din consolă.	Installation Packages / Relay	GravityZone Business Security Enterprise	Control Center creează pachete modulare și permite instalare manuală sau remote prin Relay. *Referințe: S19, S01*	**Conform**
R-098	Consola trebuie să afișeze nume, IP, OS, module, politică și actualizări pentru fiecare endpoint.	Network inventory / Endpoint details	GravityZone Business Security Enterprise	Inventarul și detaliile endpointurilor afișează identificare, OS, rețea, politică, protecție și versiuni. *Referințe: S16, S04*	**Conform**
R-099	Trebuie să existe kit universal 32/64-bit, fizic/VDI, web installer/full.	Installation Packages / BEST	GravityZone Business Security Enterprise	Pachetele de instalare se generează atât ca downloader (kit redus, care descarcă automat componentele potrivite arhitecturii 32 sau 64 de biți a mașinii), cât și ca kit complet offline. Pachetul se configurează cu modulele necesare și cu profilul de scanare adaptat mașinilor fizice și celor virtuale/VDI. *Referințe: S19*	**Conform**
R-100	Administratorul trebuie să configureze acțiuni implicite și alternative pentru fișiere infectate: deny access, disinfect, delete, quarantine sau no action.	Antimalware — acțiuni on-access / on-demand	GravityZone Business Security Enterprise	Politica Antimalware permite configurarea independentă a acțiunii implicite și a acțiunii alternative pentru fișierele infectate, din opțiunile: interzice accesul, dezinfectează, șterge, mută în carantină și nicio acțiune. *Referințe: S28*	**Conform**
R-101	Administratorul trebuie să configureze acțiuni implicite și alternative pentru fișiere suspecte: deny access, delete, quarantine sau no action.	Antimalware — acțiuni on-access / on-demand	GravityZone Business Security Enterprise	Politica Antimalware permite configurarea independentă a acțiunii implicite și a acțiunii alternative pentru fișierele suspecte, din opțiunile: interzice accesul, șterge, mută în carantină și nicio acțiune. *Referințe: S28*	**Conform**
R-102	Scanarea on-access și on-demand trebuie să permită excluderi pe directoare, discuri, fișiere, extensii și procese.	Antimalware / Network Protection	GravityZone Business Security Enterprise	Antimalware oferă scanare on-access/on-demand, acțiuni configurabile, excluderi, arhive, semnături, ML/AI și protecție web. *Referințe: S28, S29, S02*	**Conform**
R-103	Trebuie configurate dimensiunea maximă a arhivei și profunzimea scanării în arhive.	Antimalware / Network Protection	GravityZone Business Security Enterprise	Antimalware oferă scanare on-access/on-demand, acțiuni configurabile, excluderi, arhive, semnături, ML/AI și protecție web. *Referințe: S28, S29, S02*	**Conform**
R-104	Trebuie să existe scanare euristică comportamentală pentru amenințări necunoscute.	Antimalware / Network Protection	GravityZone Business Security Enterprise	Antimalware oferă scanare on-access/on-demand, acțiuni configurabile, excluderi, arhive, semnături, ML/AI și protecție web. *Referințe: S28, S29, S02*	**Conform**
R-105	Trebuie scanate suporturi precum CD, hard disk extern și unități partajate.	Antimalware / Network Protection	GravityZone Business Security Enterprise	Antimalware oferă scanare on-access/on-demand, acțiuni configurabile, excluderi, arhive, semnături, ML/AI și protecție web. *Referințe: S28, S29, S02*	**Conform**
R-106	Trebuie scanate automat emailurile POP3/SMTP la nivelul stației.	Email Traffic Scan / Network Protection	GravityZone Business Security Enterprise	Politicile includ Email Traffic Scan și scanare SMTP. Suportul exact POP3/SMTP, porturi și clienți trebuie demonstrat pe versiunea agentului și în contextul TLS. *Referințe: S40*	**Conform**
R-107	Trebuie configurate căile scanate la cerere.	Antimalware / Network Protection	GravityZone Business Security Enterprise	Antimalware oferă scanare on-access/on-demand, acțiuni configurabile, excluderi, arhive, semnături, ML/AI și protecție web. *Referințe: S28, S29, S02*	**Conform**
R-108	Trebuie oferită protecție anti-spyware prin semnături și euristică.	Antimalware / Network Protection	GravityZone Business Security Enterprise	Motorul antimalware oferă protecție anti-spyware prin mecanisme de detecție bazate pe semnături și pe analiză euristică, completate de tehnologii de machine learning, în conformitate cu cerința caietului de sarcini. *Referințe: S28, S29, S02*	**Conform**
R-109	Trebuie setată prioritatea scanărilor programate.	Antimalware On-Demand	GravityZone Business Security Enterprise	Task-urile de scanare programată permit configurarea priorității de execuție și a impactului asupra resurselor endpoint-ului (nivel redus, mediu sau ridicat), astfel încât scanările să fie ordonate în funcție de criticitatea sistemului protejat. *Referințe: S20, S28*	**Conform**
R-110	Mecanismele de scanare trebuie configurate local, cloud sau hibrid	Antimalware / Network	GravityZone Business	Antimalware oferă scanare on-access/on-demand, acțiuni configurabile local,	**Conform**

	pentru optimizarea performanței.	Protection	Security Enterprise	cloud sau hibrid, excluderi, arhive, semnături, ML/AI și protecție web. *Referințe: S28, S29, S02*	
R-111	Trebuie suportate detecții pe semnături, comportamentul fișierelor și monitorizarea proceselor.	Antimalware / Network Protection	GravityZone Business Security Enterprise	Antimalware oferă scanare on-access/on-demand, acțiuni configurabile, excluderi, arhive, semnături, ML/AI și protecție web. *Referințe: S28, S29, S02*	**Conform**
R-112	Trebuie scanate paginile web și oferit antiphishing.	Antimalware / Network Protection	GravityZone Business Security Enterprise	Antimalware oferă scanare on-access/on-demand, acțiuni configurabile, excluderi, arhive, semnături, ML/AI și protecție web. *Referințe: S28, S29, S02*	**Conform**
R-113	Trebuie setată parolă pentru protecția la dezinstalare.	BEST — protecție la dezinstalare	GravityZone Business Security Enterprise	Politica permite setarea unei parole obligatorii pentru dezinstalarea sau modificarea agentului de securitate pe endpoint. *Referințe: S19, S20*	**Conform**
R-114	Linux trebuie protejat în timp real conform kernelului instalat.	BEST for Linux — protecție on-access	GravityZone Business Security Enterprise	Agentul pentru Linux asigură protecție în timp real (on-access), folosind fanotify sau modulul DazukoFS în funcție de versiunea de kernel a distribuției instalate. *Referințe: S05*	**Conform**
R-115	VDI persistent/non-persistent trebuie suportat prin Golden Image/Template.	Security for Virtualized Environments / Golden Image	Security for Virtualized Environments (VDI/VS)	GravityZone oferă acțiuni Mark/Unmark as Golden Image; documentația SVE descrie instalarea în template/VDI și protecția VM-urilor non-persistente. *Referințe: S09, S10*	**Conform**
R-116	Modulul ML/euristic avansat trebuie să clasifice atacul, să configureze report/monitor/block, sensibilitate și acțiuni distincte pentru fișier/rețea.	HyperDetect + Network Attack Defense	GravityZone Business Security Enterprise	Modulul HyperDetect clasifică tipul de atac, permite selectarea acțiunii aplicate (raportare, monitorizare sau blocare), configurarea nivelului de sensibilitate pe fiecare categorie de amenințare și tratarea diferențiată a amenințărilor de tip fișier față de cele venite prin rețea, împreună cu Network Attack Defense. *Referințe: S03, S28*	**Conform**
R-117	Firewall-ul trebuie să configureze reguli pentru aplicații sau conectivitate.	Firewall	GravityZone Business Security Enterprise	Firewall-ul gestionează reguli și profiluri pe rețele/adaptoare, inclusiv Trusted, Home/Office, Public și Untrusted. *Referințe: S44, S02*	**Conform**
R-118	Firewall-ul trebuie să poată fi instalat, activat, dezactivat și dezinstalat.	Firewall	GravityZone Business Security Enterprise	Firewall-ul gestionează reguli și profiluri pe rețele/adaptoare, inclusiv Trusted, Home/Office, Public și Untrusted. *Referințe: S44, S02*	**Conform**
R-119	Firewall-ul trebuie să definească rețele de încredere.	Firewall	GravityZone Business Security Enterprise	Firewall-ul gestionează reguli și profiluri pe rețele/adaptoare, inclusiv Trusted, Home/Office, Public și Untrusted. *Referințe: S44, S02*	**Conform**
R-120	Data Protection trebuie să blocheze date confidențiale transmise prin HTTP sau SMTP pe baza unor reguli.	Content Control - Data Protection	GravityZone Business Security Enterprise	CERINȚĂ EXCLUSĂ DIN CAIETUL DE SARCINI de către entitatea contractantă, prin clarificările publicate în 05.08.2026 și 06.08.2026, funcționalitatea de tip DLP fiind considerată o categorie distinctă de soluții. Prin urmare nu face obiectul prezentei oferte. Menționăm că GravityZone include modulul Content Control – Data Protection, care poate fi activat ulterior la solicitarea beneficiarului. *Referințe: Clarificare entitate contractantă 05.08.2026 (DLP) și 06.08.2026 (Data Protection)*	**Cerință exclusă**
R-121	Content Control trebuie să blocheze Internetul pe mașini sau grupuri și pe intervale orare.	Content Control / Web Access Control / Application Blacklisting	GravityZone Business Security Enterprise	Web Access Control permite reguli allow/block/warn, categorii, URL-uri și programe orare; Application Blacklisting controlează aplicații. *Referințe: S40, S41*	**Conform**
R-122	Content Control trebuie să blocheze pagini după cuvinte cheie și să permită doar pagini definite de administrator.	Content Control / Web Access Control	GravityZone Business Security Enterprise	Modulul Content Control asigură blocarea accesului la Internet pe mașini și grupuri, pe intervale orare configurabile, filtrarea pe categorii de conținut predefinite, blocarea sau permiterea adreselor web pe baza unor reguli cu cuvinte-cheie și expresii în URL, precum și regimul de acces exclusiv la paginile definite de administrator (listă de permitere). *Referințe: S40, S41*	**Conform**
R-123	Content Control trebuie să blocheze aplicații definite de administrator.	Content Control / Web Access Control / Application Blacklisting	GravityZone Business Security Enterprise	Web Access Control permite reguli allow/block/warn, categorii, URL-uri și programe orare; Application Blacklisting controlează aplicații. *Referințe: S40, S41*	**Conform**
R-124	Content Control trebuie să restricționeze site-uri după categorii precum dating, violență și pornografie.	Content Control / Web Access Control / Application Blacklisting	GravityZone Business Security Enterprise	Web Access Control permite reguli allow/block/warn, categorii, URL-uri și programe orare; Application Blacklisting controlează aplicații. *Referințe: S40, S41*	**Conform**
R-125	Device Control trebuie să poată fi instalat/dezinstalat conform setărilor.	Device Control	GravityZone Business Security Enterprise	Device Control se instalează/reconfigurează modular și aplică reguli și excluderi pe clase de dispozitive. *Referințe: S42, S43*	**Conform**

R-126	Device Control trebuie să controleze Bluetooth, CDROM, floppy, IEEE 1284.4/1394, imaging, modem, tape, portable, COM/LPT, SCSI RAID, imprimante, adaptoare și storage.	Device Control	GravityZone Business Security Enterprise	Device Control acoperă clasele de dispozitive solicitate — Bluetooth, unități CD/DVD-ROM, unități de stocare internă și externă, dispozitive de imagistică, modemuri, unități pe bandă, dispozitive portabile Windows, porturi COM/LPT, controlere SCSI RAID, imprimante și adaptoare de rețea cablate și wireless — cu permisiuni (blocat / doar citire / permis) și excluderi configurabile per clasă și per dispozitiv individual. *Referințe: S42, S43*	**Conform**
R-127	Device Control trebuie să configureze permisiuni și excluderi pentru dispozitive.	Device Control	GravityZone Business Security Enterprise	Device Control se instalează/reconfigurează modular și aplică reguli și excluderi pe clase de dispozitive. *Referințe: S42, S43*	**Conform**
R-128	Power User trebuie să poată fi instalat/dezinstalat.	Power User	GravityZone Business Security Enterprise	Power User oferă drepturi locale controlate, iar administratorul din Control Center poate suprascrie setările. *Referințe: S01*	**Conform**
R-129	Power User trebuie să acorde utilizatorilor dreptul de a modifica setările locale ale agentului.	Power User	GravityZone Business Security Enterprise	Power User oferă drepturi locale controlate, iar administratorul din Control Center poate suprascrie setările. *Referințe: S01*	**Conform**
R-130	Administratorul trebuie să poată suprascrie setările Power User din consolă.	Power User	GravityZone Business Security Enterprise	Power User oferă drepturi locale controlate, iar administratorul din Control Center poate suprascrie setările. *Referințe: S01*	**Conform**
R-131	Soluția trebuie să detecteze drivere vulnerabile și atacuri avansate de dezactivare a agentului.	Anti-tampering	GravityZone Business Security Enterprise	Anti-tampering detectează vulnerable drivers și callback evasion și permite report, deny/remediate, isolate și reboot, în funcție de tehnologie. *Referințe: S45*	**Conform**
R-132	Detectarea driverelor vulnerabile trebuie să fie compatibilă cu Windows și Linux.	Anti-Tampering	GravityZone Business Security Enterprise	Modulul Anti-Tampering asigură protecția integrității agentului de securitate pe endpoint-urile administrate, cu detecția driverelor vulnerabile și a tentativelor de evaziune prin eliminarea callback-urilor, oferind acțiuni de raportare, blocare și remediere, izolare și repornire. *Referințe: S45, S03*	**Conform**
R-133	Soluția trebuie să detecteze eliminarea sau dezactivarea malițioasă a callback-urilor agentului și accesul neautorizat la kernel.	Anti-tampering	GravityZone Business Security Enterprise	Anti-tampering detectează vulnerable drivers și callback evasion și permite report, deny/remediate, isolate și reboot, în funcție de tehnologie. *Referințe: S45*	**Conform**
R-134	Criptarea pentru 1.000 de entități trebuie administrată din aceeași consolă ca protecția antivirus.	Full Disk Encryption	Full Disk Encryption — 1 000 entități	GravityZone gestionează BitLocker, FileVault/diskutil din Control Center și stochează cheile de recuperare. *Referințe: S38, S39*	**Conform**
R-135	Produsul trebuie să folosească BitLocker pentru Windows și FileVault pentru macOS.	Full Disk Encryption	Full Disk Encryption — 1 000 entități	GravityZone gestionează BitLocker, FileVault/diskutil din Control Center și stochează cheile de recuperare. *Referințe: S38, S39*	**Conform**
R-136	Consola trebuie să ofere vizibilitate asupra numelui, IP, OS, volum/partiție, stare, tip, mărime și recovery key ID.	Full Disk Encryption	Full Disk Encryption — 1 000 entități	GravityZone gestionează BitLocker, FileVault/diskutil din Control Center și stochează cheile de recuperare. *Referințe: S38, S39*	**Conform**
R-137	Criptarea trebuie suportată pe Windows 7/10/11 Pro/Enterprise cu TPM, Windows Server 2012/2012 R2/2016/2019/2022 cu TPM și macOS 10.12+.	BEST for macOS / Full Disk Encryption	GravityZone Business Security Enterprise + Full Disk Encryption	Full Disk Encryption asigură criptarea prin gestionarea centralizată a tehnologiilor native BitLocker (Windows) și FileVault (macOS), pentru edițiile Windows Pro și Enterprise și Windows Server, cu și fără TPM, precum și pentru macOS. Conform clarificării entității contractante din 06.08.2026, este obligatorie compatibilitatea cu sistemele de operare aflate în perioada de suport activ, iar compatibilitatea cu versiunile End-of-Life (Windows 7, Windows Server 2012 și 2012 R2, macOS 10.12) este acceptată fără a fi obligatorie. *Referințe: S38, S39, Clarificare entitate contractantă 06.08.2026*	**Conform**

SURSE OFICIALE CITATE

S01. Arhitectura GravityZone, Control Center, BEST, Relay, Power User, Security Server — https://www.bitdefender.com/business/support/en/77209-392421-understanding-gravityzone-architecture.html

S02. Caracteristici pe tip de endpoint și scanare centrală — https://www.bitdefender.com/business/support/en/77209-376324-features-by-asset-type.html

S03. Caracteristici de securitate și add-on-uri pe produs — https://www.bitdefender.com/business/support/en/77209-1441675-security-features.html

S04. Caracteristici operaționale pe produs — https://www.bitdefender.com/business/support/en/77209-1441676-operational-features.html

S05. Cerințe și sisteme de operare pentru endpoint protection — https://www.bitdefender.com/business/support/en/77209-376327-endpoint-protection.html

S06. Sisteme Windows legacy și limitările add-on-ului — https://www.bitdefender.com/business/support/en/77211-1476312-best-for-windows-legacy-endpoints.html

S07. Anunț GravityZone Support for Windows Legacy Systems — https://www.bitdefender.com/business/support/en/71263-1469802-gravityzone-support-for-windows-legacy-systems.html
S08. GravityZone virtual appliance și formatele VMware/Citrix/Hyper-V — https://www.bitdefender.com/business/support/en/77212-376338-gravityzone-virtual-appliance.html
S09. Security for Virtualized Environments - datasheet — https://download.bitdefender.com/resources/media/materials/business/en/Bitdefender_GravityZone_SVE_DataSheet_A4_en_EN_v01_screen.pdf
S10. Release notes GravityZone Control Center, inclusiv Golden Image și update staging — https://www.bitdefender.com/business/support/en/77209-78199-gravityzone-control-center.html
S11. Update staging și inele Test/Production — https://www.bitdefender.com/business/support/en/77209-952349-update-staging.html
S12. Actualizarea GravityZone on-premises și staging — https://www.bitdefender.com/business/support/en/77212-90377-update-gravityzone.html
S13. Dashboard și portlet-uri configurabile — https://www.bitdefender.com/business/support/en/77212-94244-dashboard.html
S14. Rapoarte configurabile, programare, formate și email — https://www.bitdefender.com/business/support/en/77209-1424532-reports.html
S15. Trimiterea rapoartelor prin email — https://www.bitdefender.com/business/support/en/77211-88557-emailing-reports.html
S16. Inventory management și inventar aplicații/patch-uri — https://www.bitdefender.com/business/support/en/77212-78783-inventory-management.html
S17. Integrarea Microsoft Active Directory — https://www.bitdefender.com/business/support/en/77209-158550-microsoft-active-directory.html
S18. Descoperirea rețelei și workgroup/domain — https://www.bitdefender.com/business/support/en/77209-157541-network-discovery-issues-in-bitdefender-gravityzone.html
S19. Instalarea agenților, inclusiv Relay și instalare remote — https://www.bitdefender.com/business/support/en/77209-157497-install-security-agents---standard-procedure.html
S20. Politici și managementul securității — https://www.bitdefender.com/business/support/en/77209-77398-security-management.html
S21. Reguli de atribuire a politicilor — https://www.bitdefender.com/business/support/en/77209-342910-assigning-local-policies.html
S22. Roluri de utilizator — https://www.bitdefender.com/business/support/en/77209-124342-user-roles.html
S23. Drepturi granulare ale utilizatorilor — https://www.bitdefender.com/business/support/en/77211-124345-user-rights.html
S24. Cont, timeout sesiune și securitate autentificare — https://www.bitdefender.com/business/support/en/77209-94051-manage-your-account.html
S25. User Activity Log — https://www.bitdefender.com/business/support/en/77212-94052-user-activity-log.html
S26. Tipuri de notificări GravityZone — https://www.bitdefender.com/business/support/en/77211-94322-notification-types.html
S27. Administrarea fișierelor în carantină — https://www.bitdefender.com/business/support/en/77211-343015-managing-the-quarantined-files.html
S28. Antimalware on-access: acțiuni, arhive și tehnologii — https://www.bitdefender.com/business/support/en/77209-342930-on-access.html
S29. Excluderi antimalware — https://www.bitdefender.com/business/support/en/77209-342987-exclusions.html
S30. Ransomware Protection / Ransomware Mitigation — https://techzone.bitdefender.com/en/security-layers/protection/ransomware-protection.html
S31. Sandbox Analyzer - analiză, IoC, MITRE, timeline — https://techzone.bitdefender.com/en/security-layers/protection/sandbox-analyzer.html
S32. Investigarea incidentelor EDR, graph, răspuns, Remote Shell — https://www.bitdefender.com/business/support/en/77209-151142-investigating-incidents.html
S33. Custom detection rules EDR — https://www.bitdefender.com/business/support/en/77209-396276-edr-custom-detection-rules.html
S34. Custom exclusion rules EDR/XDR — https://www.bitdefender.com/business/support/en/77209-396279-custom-exclusion-rules.html
S35. Blocklist și import hash MD5/SHA256 prin CSV — https://www.bitdefender.com/business/support/en/77209-151159-edr-blocklist.html
S36. Patch Management — https://www.bitdefender.com/business/support/en/77209-376316-patch-management.html
S37. Risk/patch inventory și aplicații instalate — https://www.bitdefender.com/business/support/en/77209-215271-patch-management-faq.html
S38. Full Disk Encryption — https://www.bitdefender.com/business/support/en/77212-376335-full-disk-encryption.html
S39. Full Disk Encryption FAQ — https://www.bitdefender.com/business/support/en/77211-63279-gravityzone-full-disk-encryption-faq.html
S40. Content Control și Data Protection HTTP/SMTP — https://www.bitdefender.com/business/support/en/77209-342965-content-control.html
S41. Categorii web și programarea accesului — https://www.bitdefender.com/business/support/en/77209-343038-web-categories-in-gravityzone-content-control.html
S42. Device Control — https://www.bitdefender.com/business/support/en/77211-376305-device-control.html
S43. Tipuri de dispozitive suportate — https://www.bitdefender.com/business/support/en/77211-342970-supported-device-types.html
S44. Firewall - rețele, profiluri și niveluri de încredere — https://www.bitdefender.com/business/support/en/77209-342961-settings.html
S45. Anti-tampering: vulnerable drivers și callback evasion — https://www.bitdefender.com/business/support/en/77212-537435-anti-tampering.html
S46. AV-TEST - rezultate Bitdefender business — https://www.av-test.org/en/antivirus/business-windows-client/manufacturer/bitdefender/
S47. AV-TEST Awards 2025 — https://www.av-test.org/en/news/av-test-awards-2025-celebrating-the-very-best-of-it-security-products/
S48. AV-Comparatives Business Security Test 2025 — https://www.av-comparatives.org/tests/business-security-test-2025-august-november/
S49. AV-Comparatives - profil Bitdefender și certificări — https://www.av-comparatives.org/vendors/bitdefender/
S52. Retenția datelor EDR și add-on-uri — https://www.bitdefender.com/business/support/en/77209-151423-retention-policies.html

Numele, prenumele: Vasilache Dionisie
În calitate de: Director
Ofertantul: „TXD IT SOLUTIONS” S.R.L., IDNO 1007600035390
Adresa: str. Mitropolit Gavriil Bănulescu-Bodoni 8, MD-2012, mun. Chișinău, Republica Moldova
Data: 12.08.2026

Digitally signed by Vasilache Dionisie
Date: 2026.08.12 09:35:22 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

_____ (Semnătura electronică) L.Ș.