AP 8937 /10.02.2023

Finanțat de Uniunea Europeană NextGenerationEU

Planul Național de Redresare și Reziliență

Anexa 1

SPECIFICAȚIILE TEHNICE CARE INDICĂ O ANUMITA ORIGINE, SURSĂ, PRODUCȚIE, UN PROCEDEU SPECIAL, O MARCĂ DE FABRICĂ SAU COMERȚ, UN BREVET DE INVENȚIE, O LICENȚĂ DE FABRICAȚIE, SUNT MENȚIONATE DOAR PENTRU IDENTIFICAREA CU UȘURINȚĂ A TIPULUI DE PRODUS ȘI NU AU CA EFECT FAVORIZAREA SAU ELIMINAREA ANUMITOR OPERATORI ECONOMICI SAU A ANUMITOR PRODUSE. ACESTE SPECIFICAȚII VOR FI CONSIDERATE CA AVÂND MENȚIUNEA "SAU ECHIVALENT"

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
1	**Echipament integrat de protectie în rețea cu capabilități de rutare**		**buc**	**2**
	Descriere generală	Echipament integrat de tip Next Generation Firewall (NGFW), cu capabilitati de rutare (statica si dinamica), firewall de tip stateful, funcționalități de inspecție a traficului de date (IPS, antivirus, filtrare pagini web, controlul aplicațiilor, antispam), terminare de tunele VPN de tip IPSec si SSL. Platforma hardware, sistemul de operare și licențele/actualizările semnăturilor de securitate trebuie să provină de la același producător (soluție integrată).		
	Specificații hardware	Pentru acuratețe și performanță, toate modulele de protectie ce alcătuiesc modulele de securitate trebuie sa funcționeze având la bază un sistem de operare dedicat, dezvoltat de către producătorul echipamentului. Nu este permisă folosirea unui sistem de operare comercial, pentru uz general. 8 interfete 10GE SFP+ 16 interfețe 1GE RJ45 8 interfețe 1GE SFP 1 interfață RJ45 de management 1 interfață RJ45 dedicată pentru funcționare HA (High Availability) 1 interfață USB 1 port consolă RJ45		
	Performanța sistemului	Capacitate trafic procesat firewall (pachete UDP de 512 octeti): 78 Gbps Capacitate trafic procesat firewall (pachete pe secundă) : 100 Mpps Capacitate trafic procesat IPSec VPN (pachete UDP de 512 octeti): 50 Gbps Capacitate trafic procesat cu inspecție SSL: 8 Gbps Capacitate trafic procesat cu inspecție IPS: 11 Gbps Număr de sesiuni concurente cu inspecție SSL: 750000 Tunele IPSec VPN Site-to-Site: 2000 Tunele IPSec VPN Client-to-Site: 45000 Capacitate trafic procesat SSL-VPN: 3,5 Gbps Sesiuni concurente (TCP): 7500000 Sesiuni noi/sec: 450000 Politici firewall: 10000 Număr de switch-uri pentru management centralizat (funcție de controller):72 Număr de AP-uri pentru management centralizat (funcție de controller): 512 Suport definire până la 10 firewall-uri virtuale (tabele separate de rutare) fără licență adițională		
	Parametrii echipament	Alimentare alternativă 100-240V, 50-60Hz, Consum maxim de putere: 195 W Sursă redundantă de alimentare de tip hot-swap		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
	Funcționalități suportate	Servicii de Rețea: ➢ suport SD-WAN ➢ suport PPPoE ➢ client/server DHCP ➢ policy-based routing ➢ rutare dinamică: RIP, OSPF ,BGP, IS-IS, Multicast ➢ suport multi-zone ➢ VLAN Tagging(802.1Q) ➢ suport pentru interfețe EMAC-VLAN Traffic shaping : ➢ suport DiffServ ➢ configurarea lățimii de bandă garantată/maximă per profil/politică ➢ traffic shaping per-IP, per-Policy Domenii virtuale: ➢ domenii firewall/rutare separate ➢ posibilitatea de folosire mixtă a domeniilor virtuale în modul transparent(bridge)/rutare High Availability: ➢ Activ/Activ, Activ/Pasiv ➢ stateful Failover ➢ link status monitor ➢ link failover Servicii de securitate firewall: ➢ filtrare în funcție de politici ➢ suport proxy explicit ➢ suport pentru SIP pinholing ➢ suport pentru server load balancing ➢ suport pentru autentificarea userilor la nivel de politici firewall prin: o bază de date locală o Windows AD o RADIUS/LDAP/TACACS+ Servicii VPN: ➢ PPTP, IPsec, SSL ➢ suport IKEv1, IKEv2 pentru IPsec ➢ suport algoritmi pentru IPsec: AES, AES GCM, SHA-256, SHA-384, SHA-512 ➢ suport IPsec NAT Traversal ➢ soluția propusă să permită stabilirea conexiunilor de tip VPN de stație atât pentru PC-uri cât și dispozitive mobile. Servicii de prevenire a intruziunilor (IPS): ➢ detecția și blocarea încercărilor de intruziune după semnături predefinite		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		➢ suport pentru crearea de semnături personalizabile pentru detecția și blocarea încercărilor de intruziune ➢ blocarea conexiunilor către servere de tip Botnet C&C, în baza reputației adreselor IP ➢ suport pentru blocarea atacurilor de tip DoS Servicii de tip Antivirus: ➢ inspecție pentru protocoalele HTTP, POP3, SMTP, IMAP, FTP, MAPI și SSH ➢ suport Content Disarm and Reconstruction (CDR) Servicii de tip Antispam: ➢ inspecție pentru protocoalele SMTP, IMAP, POP3, MAPI Servicii de tip Application Control: ➢ identificarea și controlul traficului la nivel de aplicație pe bază de semnături (indiferent de protocol) ➢ traffic shaping (per aplicație) ➢ suport inspecție trafic SSL Servicii filtrare a paginilor web (Web Filtering): ➢ blocarea accesului utilizatorilor la pagini web, folosind o bază de date actualizată în mod automat, ce clasifică paginile web la nivel global, în diferite categorii, în funcție de conținutul acestora ➢ posibilitatea de modificare locală a clasificarii paginilor web în alte categorii decât cele din baza de date actualizată în mod automat ➢ posibilitatea definirii de liste statice cu URL-uri permise/blocate Functionalitati de tip controller pentru switch-uri si access point-uri: ➢ posibilitatea de a funcționa ca switch și access point controller Servicii de identificare a device-urilor din rețea: ➢ colectarea informațiilor device-urilor conectate la rețea precum adresa MAC, adresa IP, sistem de operare, hostname, username		
	Management, logare și raportare	Administrare: ➢ configurare prin CLI (consola, telnet, SSH) ➢ configurare prin Web UI ➢ definire utilizatori/administratori cu drepturi configurabile ➢ suport Syslog ➢ suport SNMP ➢ backup configurație (configurația echipamentului trebuie să se poată exporta într-un fișier text) Logare centralizată prin intermediul unei platforme dedicate (mașină virtuală) ce asigură următoarele funcționalități: ➢ poate fi instalată pe un mediu de virtualizare VMware, Microsoft Hyper-V sau KVM ➢ colectarea centralizată a log-urilor ce sunt raportate de către echipamentele deservite		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		➢ posibilitatea de generare de rapoarte ce pot fi personalizate Servicii de autentificare a utilizatorilor/administratorilor: ➢ prin baza de date locală ➢ prin Windows AD ➢ prin LDAP/RADIUS/TACACS+ ➢ suport pentru autentificarea prin doi factori ➢ restrictionare acces după adresa IP		
	Software	Licențe pentru activarea actualizărilor serviciilor: antivirus, antispam, prevenirea intruziunilor (IPS), filtrare pagini web (Web Filtering) Licență pentru activarea platformei dedicate de logare centralizată, sub forma de masina virtuală, de tip perpetuă, cu capabilitate de procesare cantitativă de 5 GB de loguri pe zi (se va instala și folosi minim o singura platformă pentru toate echipamentele de tip NGFW)		
	Service și garanție	Soluția va beneficia de **minim 2 ani** de suport ce va include: ➢ înlocuirea echipamentului în caz de defecțiune hardware ➢ suport tehnic din partea vendorului 7 zile pe săptămână, 24 ore pe zi, atât pentru echipamentul de tip NGFW, cât și pentru platforma de logare centralizată ➢ actualizare firmware, cu versiuni minore și majore ➢ actualizare automată de semnături de securitate pentru îndeplinirea tuturor funcționalităților cerute mai sus După expirarea serviciilor achizitionate, echipamentul trebuie să funcționeze, să permită atât administrarea cât și fluxurile de date, chiar dacă semnăturile nu mai sunt actualizate la zi.		
2	**Echipament de comunicatii tip 1**		**buc**	**21**
	Configurație Hardware	24 interfețe 10/100/1000 Ethernet RJ45 PoE (802.3af/at) Buget PoE: 370W 4 interfete SFP+, dintre care 1 interfețe echipate cu transceivere de tip SFP SX, de la același producător sau recomandate de producătorul echipamentului 1 interfață serial RJ-45 de consolă Montabil în rack, dimensiune: 1RU		
	Caracteristici	Capacitate de switching: 128 Gbps Trafic măsurat în pachete pe secundă: 190 Mpps Capacitate tabela de adrese MAC: 32000 Latență: < 1µs Suport pentru 4000 VLAN-uri Link Aggregation Group Size: 8 Total Link Aggregation Groups: 16 ACL: 768 Instanțe Spanning Tree: 16 Packet Buffers: 2 MB Memorie DRAM: 512 MB Memorie FLASH: 64M		
	Functionalități generale	Suport LAG min-max bundle Suport IGMP snooping, IGMP proxy și IGMP querier Suport LLDP transmit, LLDP-MED, LLDP-MED ELIN Suport Sticky MAC Suport STP root guard și STP BPDU guard Suport Rapid PVST interoperation Suport Storm control și Per-port storm control Suport Global burst-size control		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		Suport Loop guard Suport SPAN port Suport Flow Control Suport 802.1p inclusive priority queuing trunk si WRED Suport diagnostic cablu cu TDR (time-domain reflectometer)		
	Funcționalități management și monitorizare a echipamentului	Management prin intermediul echipamentului NGFW (cu rol de controller) ofertat, cu funcționalități de configurare a parametrilor de funcționare și actualizare firmware, în mod centralizat (inclusiv funcționalități de carantinare a stațiilor conectate, funcționalități de tip network access control (NAC)) Management prin Telnet / SSH Suport pentru download, upload de software prin FTP/TFTP sau interfață grafică Suport SNMPv3		
	Funcționalități Securitate	Suport 802.1X port mode Suport 802.1X MAC-based Mode Suport User-based (802.1X) VLAN assignment Suport 802.1X MAB Suport 802.1X open-auth mode Suport RADIUS accounting server Suport pentru RADIUS CoA și mesaje de deconectare Suport EAP pass-through Suport DHCP snooping Suport Flap Guard Suport Dynamic ARP Inspection (IPv4)		
	Condiții de alimentare	Alimentare curent alternativ 100-240V, 50-60 Hz Consum maxim de putere: 470 W		
	Certificări, condiții de mediu și utilizare	Certificari: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 Temperatură de operare: 0 - 45 grade Celsius Umiditate: 10 – 90 %, fără condens MTBF (Mean Time Between Failures): minim 10 ani		
	Garanție	Soluția va beneficia de **minim 2 ani** de suport ce vor include: ➢ înlocuirea echipamentului în caz de defecțiune hardware cu termen remediere maxim 3 zile lucrătoare ➢ suport tehnic din partea furnizorului minim 7 zile pe saptamana, 24 ore pe zi ➢ update firmware, versiuni majore și minore (patch)		
3	**Echipament de comunicatii tip 2**		**buc**	**1**
	Configurație Hardware	24 interfețe 10/100/1000 Ethernet RJ45 4 interfete SFP+ 1 interfață serial RJ-45 de consolă Montabil în rack, dimensiune: 1RU		
	Caracteristici	Capacitate de switching: 128 Gbps Trafic măsurat în pachete pe secundă: 190 Mpps Capacitate tabela de adrese MAC: 32000 Latență: < 1µs Suport pentru 4000 VLAN-uri Link Aggregation Group Size: 8 Total Link Aggregation Groups: 16 ACL: 768 Instanțe Spanning Tree: 16 Packet Buffers: 2 MB Memorie DRAM: 512 MB Memorie FLASH: 64M		
	Funcționalități generale	Suport LAG min-max bundle Suport IGMP snooping, IGMP proxy și IGMP querier Suport LLDP transmit, LLDP-MED, LLDP-MED ELIN Suport Sticky MAC Suport STP root guard și STP BPDU guard Suport Rapid PVST interoperation		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		Suport Storm control și Per-port storm control Suport Global burst-size control Suport Loop guard Suport SPAN port Suport Flow Control Suport 802.1p inclusive priority queuing trunk si WRED Suport diagnostic cablu cu TDR (time-domain reflectometer)		
	Funcționalități management și monitorizare a echipamentului	Management prin intermediul echipamentului de tip NGFW (cu rol de controller) ofertat, cu funcționalități de configurare a parametrilor de funcționare și actualizare firmware, în mod centralizat (inclusiv funcționalități de carantinare a stațiilor conectate, funcționalități de tip network access control (NAC)) Management prin interfață grafică în mod stand alone Management prin interfața de tip linie de comanda (CLI) în mod stand alone Management prin Telnet / SSH Suport pentru download, upload de software prin FTP/TFTP sau interfața grafică Suport SNMPv3		
	Funcționalități Securitate	Suport 802.1X port mode Suport 802.1X MAC-based Mode Suport User-based (802.1X) VLAN assignment Suport 802.1X MAB Suport 802.1X open-auth mode Suport RADIUS accounting server Suport pentru RADIUS CoA și mesaje de deconectare Suport EAP pass-through Suport DHCP snooping Suport Flap Guard Suport Dynamic ARP Inspection (IPv4)		
	Condiții de alimentare	Alimentare curent alternativ 100-240V, 50-60 Hz Consum maxim de putere: 30 W		
	Certificări, condiții de mediu și utilizare	Certificări: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 Temperatură de operare: 0 - 45 grade Celsius Umiditate: 10 – 90 %, fără condens MTBF (Mean Time Between Failures): minim 10 ani		
	Garanție	Soluția va beneficia de **minim 2 ani** de suport ce vor include: ➢ înlocuirea echipamentului în caz de defecțiune hardware cu termen remediere maxim 3 zile lucrătoare ➢ suport tehnic din partea furnizorului minim 7 zile pe săptămână, 24 ore pe zi ➢ update firmware, versiuni majore și minore (patch)		
4	**Echipament de comunicatii tip 3**		**buc**	**9**
	Configurație Hardware	48 interfețe 10/100/1000 Ethernet RJ45 4 interfete SFP+, dintre care 2 interfețe echipate cu transceivere de tip SFP SX, de la același producător sau recomandate de producătorul echipamentului 1 interfața serial RJ-45 de consolă Montabil în rack, dimensiune: 1RU		
	Caracteristici	Capacitate de switching: 176 Gbps Trafic măsurat în pachete pe secundă: 260 Mpps Capacitate tabela de adrese MAC: 32000 Latență: < 1µs Suport pentru 4000 VLAN-uri Link Aggregation Group Size: 8 Total Link Aggregation Groups: 16 ACL: 768 Instanțe Spanning Tree: 16 Packet Buffers: 2 MB Memorie DRAM: 512 MB Memorie FLASH: 64M		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
	Funcționalități generale	Suport LAG min-max bundle Suport IGMP snooping, IGMP proxy şi IGMP querier Suport LLDP transmit, LLDP-MED, LLDP-MED ELIN Suport MAC learning limit Suport Sticky MAC Suport STP root guard şi STP BPDU guard Suport Rapid PVST interoperation Suport Storm control şi Per-port storm control Suport Global burst-size control Suport Loop guard Suport SPAN port Suport Flow Control Suport 802.1p inclusive priority queuing trunk si WRED Suport diagnostic cablu cu TDR (time-domain reflectometer)		
	Funcționalități management și monitorizare a echipamentului	Management prin intermediul echipamentului de tip NGFW (cu rol de controller) ofertat, cu funcționalități de configurare a parametrilor de funcționare și actualizare firmware, în mod centralizat (inclusiv funcționalități de carantinare a stațiilor conectate, funcționalități de tip network access control (NAC)); Management prin Telnet / SSH; Suport pentru download, upload de software prin FTP/TFTP sau interfață grafică; Suport SNMPv3		
	Funcționalități Securitate	Suport 802.1X port mode Suport 802.1X MAC-based Mode Suport User-based (802.1X) VLAN assignment Suport 802.1X MAB Suport 802.1X open-auth mode Suport RADIUS accounting server Suport pentru RADIUS CoA și mesaje de deconectare Suport EAP pass-through Suport DHCP snooping Suport Flap Guard Suport sFlow (IPv4) Suport Dynamic ARP Inspection (IPv4)		
	Condiții de alimentare	Alimentare curent alternativ 100-240V, 50-60 Hz Consum maxim de putere: 60 W		
	Certificări, condiții de mediu și utilizare	Certificari: FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 Temperatură de operare: 0 - 45 grade Celsius Umiditate: 10 – 90 %, fără condens MTBF (Mean Time Between Failures): minim 10 ani		
	Garanție	Soluția va beneficia de **minim 2 ani** de suport ce vor include: ➢ înlocuirea echipamentului în caz de defecțiune hardware cu termen remediere maxim 3 zile lucrătoare ➢ suport tehnic din partea furnizorului minim 7 zile pe săptămână, 24 ore pe zi ➢ update firmware, versiuni majore și minore (patch)		
5	**Echipament de comunicatii tip 4**		**buc**	**2**
	Configurație Hardware	24 interfețe GE/10GE SFP+, dintre care 12 interfețe echipate cu transceivere de tip SFP SX, 5 interfețe echipate cu transceivere de tip Gigabit Ethernet RJ45, 5 interfețe echipate cu transceivere de tip SFP+SR, și 2 interfețe echipate cu transceivere de tip SFP+ LR, transcieverele fiind de la același producător sau recomandate de producătorul echipamentului 2 interfețe 40GE/100GE QSFP+ /QSFP28 1 interfață serial RJ-45 de consolă 1 port management Montabil în rack, dimensiune: 1RU		
	Caracteristici	Capacitate de switching: 880 Gbps Trafic măsurat în pachete pe secundă: 1300 Mpps Capacitate tabelă de adrese MAC: 64000		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		Latență: 1µs Suport pentru 4000 VLAN-uri Link Aggregation Group Size: 24 Total Link Aggregation Groups: 24 Queues/port: 8 Packet Buffers: 8 MB Memorie DRAM: 8 GB Memorie FLASH: 32 MB		
	Functionalităti generale	Suport MCLAG (multichassis link aggregation) Suport MCLAG pentru STP, IGMP snooping Suport LAG min-max bundle Suport IGMP snooping, IGMP proxy și IGMP querier Suport LLDP transmit, LLDP-MED, LLDP-MED: ELIN Suport Sticky MAC Suport IP-MAC binding (IPv4) Suport STP root guard și STP BPDU guard Suport Rapid PVST interoperation Suport Storm control și Per-port storm control Suport Percentage rate control Suport RSPAN si ERSPAN (IPv4) Suport Global burst-size control Suport Loop guard Suport SPAN port Suport Flow Control Suport QoS egress priority tagging (IPv4/IPv6) Suport QoS ECN (IPv4/IPv6) Suport 802.1p, inclusiv priority queuing trunk si WRED Suport QoS queue counters		
	Funcționalități management și monitorizare a echipamentului	Management prin intermediul echipamentului de tip NGFW (cu rol de controller) ofertat, cu funcționalități de configurare a parametrilor de funcționare și actualizare firmware, în mod centralizat (inclusiv funcționalități de carantinare a stațiilor conectate, funcționalități de tip network access control (NAC)) Management prin Telnet / SSH Suport pentru download, upload de software prin FTP/TFTP sau interfața grafică Suport SNMPv3 PTP transparent clock (IPv4/IPv6)		
	Funcționalități Securitate	Suport 802.1X port mode Suport 802.1X MAC-based Mode Suport User-based (802.1X) VLAN assignment Suport 802.1X MAB Suport open-auth mode Suport RADIUS accounting server Suport pentru RADIUS CoA și mesaje de deconectare Suport EAP pass-through Suport sFlow (IPv4) Suport Flow export (IPv4) Suport DHCP snooping Suport captura pachete Suport Flap Guard Suport Dynamic ARP Inspection (IPv4)		
	Condiții de alimentare	Alimentare curent alternativ 100-240V, 50-60 Hz Consum maxim de putere: 180 W Sursa alimentare dual		
	Certificări, condiții de mediu și utilizare	FIPS 140-2 (Level 2) support FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 Temperatură de operare: 0 - 40 grade Celsius Umiditate: 10 – 90 %, fără condens MTBF (Mean Time Between Failures): minim 10 ani		
	Garanție	Soluția va beneficia **de minim 2 ani** de suport ce vor include:		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		➢ înlocuirea echipamentului în caz de defecțiune hardware cu termen remediere maxim 3 zile lucrătoare ➢ suport tehnic din partea furnizorului 7 zile pe săptămână, 24 ore pe zi ➢ update firmware, versiuni majore și minore (patch)		
6	**Echipament de comunicatii tip 5**		**buc**	**2**
	Configurație Hardware	24 interfețe GE/10GE SFP+, dintre care 12 interfețe echipate cu transceivere de tip SFP SX, 5 interfețe echipate cu transceivere de tip Gigabit Ethernet RJ45, 5 interfețe echipate cu transceivere de tip SFP+SR, și 2 interfețe echipate cu transceivere de tip SFP+ LR, transcieverele fiind de la același producător sau recomandate de producătorul echipamentului 2 interfețe 40GE/100GE QSFP+ /QSFP28 1 interfață serial RJ-45 de consolă 1 port management Montabil în rack, dimensiune: 1RU		
	Caracteristici	Capacitate de switching: 880 Gbps Trafic măsurat în pachete pe secundă: 1300 Mpps Capacitate tabelă de adrese MAC: 64000 Latență: 1µs Suport pentru 4000 VLAN-uri Link Aggregation Group Size: 24 Total Link Aggregation Groups: 24 Queues/port: 8 Packet Buffers: 8 MB Memorie DRAM: 8 GB Memorie FLASH: 32 MB		
	Functionalităti generale	Suport MCLAG (multichassis link aggregation) Suport MCLAG pentru STP, IGMP snooping Suport LAG min-max bundle Suport IGMP snooping, IGMP proxy și IGMP querier Suport LLDP transmit, LLDP-MED, LLDP-MED: ELIN Suport Sticky MAC Suport IP-MAC binding (IPv4) Suport STP root guard și STP BPDU guard Suport Rapid PVST interoperation Suport Storm control și Per-port storm control Suport Percentage rate control Suport RSPAN si ERSPAN (IPv4) Suport Global burst-size control Suport Loop guard Suport SPAN port Suport Flow Control Suport QoS egress priority tagging (IPv4/IPv6) Suport QoS ECN (IPv4/IPv6) Suport 802.1p, inclusiv priority queuing trunk si WRED Suport QoS queue counters		
	Funcționalități management și monitorizare a echipamentului	Management prin intermediul echipamentului de tip NGFW (cu rol de controller) ofertat, cu funcționalități de configurare a parametrilor de funcționare și actualizare firmware, în mod centralizat (inclusiv funcționalități de carantinare a stațiilor conectate, funcționalități de tip network access control (NAC)) Management prin Telnet / SSH Suport pentru download, upload de software prin FTP/TFTP sau interfața grafică Suport SNMPv3 PTP transparent clock (IPv4/IPv6)		
	Funcționalități Securitate	Suport 802.1X port mode Suport 802.1X MAC-based Mode Suport User-based (802.1X) VLAN assignment Suport 802.1X MAB Suport open-auth mode		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		Suport RADIUS accounting server Suport pentru RADIUS CoA și mesaje de deconectare Suport EAP pass-through Suport sFlow (IPv4) Suport Flow export (IPv4) Suport DHCP snooping Suport captura pachete Suport Flap Guard Suport Dynamic ARP Inspection (IPv4)		
	Condiții de alimentare	Alimentare curent alternativ 100-240V, 50-60 Hz Consum maxim de putere: 180 W Sursa alimentare duală		
	Certificări, condiții de mediu și utilizare	FIPS 140-2 (Level 2) support FCC, CE, RCM, VCCI, BSMI, UL, CB, RoHS2 Temperatură de operare: 0 - 40 grade Celsius Umiditate: 10 – 90 %, fără condens MTBF (Mean Time Between Failures): minim 10 ani		
	Garanție	Soluția va beneficia **de minim 2 ani** de suport ce vor include: ➢ înlocuirea echipamentului în caz de defecțiune hardware cu termen remediere maxim 3 zile lucrătoare ➢ suport tehnic din partea furnizorului 7 zile pe săptămână, 24 ore pe zi ➢ update firmware, versiuni majore și minore (patch)		
7	**Echipament de comunicatii tip 6**		**buc**	**30**
	Caracteristici	Număr de radiouri: 3 Număr de antene: 3 antene Wi-Fi interne + 1 antena BLE/ZigBee Capabilitati Radio 1: ➢ Banda de frecvențe: 2.4 GHz ➢ Lățimea de bandă a canalelor: 20/40MHz ➢ Scheme de modulație: BPSK, QPSK, 64/256/1024 QAM ➢ Lanțuri MIMO: 2x2 Capabilitati Radio 2: ➢ Banda de frecvențe: 5.0 GHz ➢ Lățimea de banda a canalelor: 20/40/80MHz ➢ Scheme de modulatie: BPSK, QPSK, 64/256/1024 QAM ➢ Lanțuri MIMO: 2x2 Capabilitati Radio 3: ➢ Benzi de frecvențe: 2.4 GHz si 5.0 GHz ➢ Lanțuri MIMO: 1x1 Rata transmisie: ➢ Radio 1: 570 Mbps ➢ Radio 2: 1201 Mbps ➢ Radio 3: folosit pentru scanare frecvențe Capacitate număr clienți simultani radio: ➢ Radio 1: 512 ➢ Radio 2: 512 Interfețe conectare:		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		➢ 2 x RJ 45 (10/100/1000) ➢ 1 x USB ➢ 1 x RS-232 RJ45 Serial Port Support Power over Ethernet (PoE): 802.3at si 802.3af Număr de SSID-uri suportate simultan: 14 Tipuri SSID suportate: Local-Bridge, Tunnel și Mesh Suport EAP: EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-FAST Autentificare user/dispozitiv: WPA, WPA2 si WPA3 cu 802.1x sau Preshared key, WEP, Web Captive Portal, MAC blocklist & allowlist Standarde IEEE: 802.11a, 802.11b, 802.11d, 802.11e, 802.11g, 802.11h,802.11i, 802.11j, 802.11k, 802.11n, 802.11r, 802.11v, 802.11w, 802.11ac, 802.11ax, 802.1Q, 802.1X, 802.3ad, 802.3af, 802.3at, 802.3az Support functionalitati 802.11: ➢ OFDMA ➢ Spatial Reuse (BSS Coloring) ➢ MU-MIMO ➢ Enhanced Target Wake Time (TWT) Capabilitati monitorizare wireless: ➢ scanare pentru detecția de stații „rogue" ➢ WIPS / WIDS ➢ captura de pachete ➢ analiza spectrală de frecvențe Timp mediu între defecțiuni: peste 10 ani Opțiuni montare: kit montare perete și tavan cu accesorii de montaj incluse în pachet Management prin intermediul echipamentului de tip NGFW (cu rol de controller) ofertat, cu functionalitati de configurare a parametrilor de funcționare și actualizare firmware, în mod centralizat		
	Condiții de mediu și alimentare	Umiditate: 5% - 90% fără condens Temperatura de operare: 00C – 500C Consum maxim de putere: 17W Conformitate cu standardul RoHS Certificare WiFi Alliance		
	Garanție și suport	Soluția va beneficia de Minim 2 ani de suport ce va include: ➢ înlocuirea echipamentului în caz de defecțiune hardware ➢ suport tehnic de tip 27x7 din partea furnizorului ➢ actualizări de software (firmware)		
8	**Echipament de stocare a datelor de tip SAN**		**buc**	**1**
	Format	Echipamentul ofertat trebuie să fie nou, de ultimă generație, fără existența unei notificări privind data de întrerupere producție sau retragere model. Cutiile de bază în care sunt instalate controlerele trebuie să aibă dimensiune maxim 4U (unități în rack) și să poată fi instalate în rack cu dimensiune standard (industry standard racks)		
	Configurație controller	Minim două controllere redundante, configurate sub forma unui cluster activ-activ, care să permită balansarea automată a încărcării între cele două controllere.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
	Nivele RAID suportate	Echipamentul ofertat trebuie să dispună de capacitate configurare RAID pentru protecția datelor stocate, cel puțin de tip 0, 1, 3, 5, 6, 10, precum și distribuit și împărțit la nivel de block pe drive-uri cu protecție împotriva defecțiunii a 2 discuri, fără pierdere de date (distributed block level striping with double parity).		
	Memorie cache	Minim 16 GB per sistem (8 GB per controller). Echipamentul de stocare ofertat trebuie să permită creșterea capacității memoriei cache utilizând SSD-uri din configurație, până la cel puțin 4TB, cel puțin pentru operațiunile de citire.		
	Protectie memorie cache	Informația din memoria cache trebuie să fie copiată în oglinda pe cele două controllere și protejată de memorii nevolatile (flash-backed cache).		
	Discuri suportate	Minim 192 discuri hot-swap de tip LFF prin folosirea de unitate de tip controller și unități de tip expansion de tip LFF. Minim 96 discuri hot-swap de tip SFF prin folosirea de unitate de tip controller și unități de tip expansion de tip SFF. Sistemul trebuie să suporte atat HDD-uri cât și SSD-uri iar acestea trebuie să poată fi intermixate în aceeași cutie de stocare. Din rațiuni de eficiență a spațiului echipamentul trebuie sa ofere posibilitatea utilizarii a cutiilor de 60 discuri LFF prin ocuparea a maxim 4U spațiu rackabil. Sistemul de stocare trebuie să suporte discuri cu criptare hardware (FIPS).		
	Discuri instalate	Minim 10 discuri SSD SAS 12Gbps 2.5" hot-swap cu capacitate de minim 1.92TB, minim 1DWPD.		
	Scalabilitate	Sistemul de stocare trebuie să poată scala la minim 3 PB		
	Performanța	În configurație maximală, obținută prin extinderea ulterioară a resurselor, echipamentul trebuie să poată livra minim 299999 IOPS pentru operații de citire aleatorii (random reads) și minimum 108999 IOPS pentru operațiuni de scriere aleatorii (random writes), utilizând blocuri de date cu dimensiune 4 KB.		
	Porturi	Minim 8x porturi pentru conectarea sistemului de stocare la servere (4 per controler), de tip 12Gb SAS. Minim 8x cabluri de minim 1m de tip Mini-SAS HD SFF-8644 pentru conectarea directă a host-urilor. Echipamentul ofertat trebuie să dispună de cel puțin 4 porturi de tip SAS 12Gb pentru expansiune.		
	Functionalitati	Sistemul de stocare trebuie să includă următoarele funcționalități: SSD read cache, snapshots (minim 128 targets upgradabil la minim 512), volume copy, thin provisioning și criptare prin utilizarea discurilor FIPS. Aceste funcționalități trebuie sa fie licentiate permanent și incluse cu sistemul de stocare, pentru capacitatea maximă instabilă. De asemenea, opțional, sistemul de stocare să suporte prin licențiere ulterioară replicare sincronă și asincronă către un echipament similar. Echipamentul ofertat trebuie să furnizeze o disponibilitate de 99,999% prin funcții de înaltă disponibilitate și redundanță la subansamble (fără "single point of failure"). Nivelul de disponibilitate trebuie să fie menționat în evidențele producătorului. Upgrade-uri firmware fără întreruperea sistemului de stocare (online).		
	Dimensiune maximă volum logic	Minim 2PB		
	Număr maxim de volume logice	Minim 512		
	Număr maxim de host-uri	Minim 256		
	Dimensiune maximă SSD read cache	4TB		
	Alimentare și răcire	Cutiile de baza în care sunt instalate controlerele cat și cutiile de expansiune trebuie să includă surse de alimentare redundante, certificate Platinum și ventilatoare redundante.		
	Componente hot-swap	Următoarele componente trebuie să poată fi înlocuite fără oprirea sistemului de stocare (hot-swap): controlere, module I/O, discuri, surse alimentare și transceivere		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
	Porturi de administrare	Minim 1x port 1 GbE (UTP, RJ-45) per controller pentru management out-of-band. Minim 2x porturi seriale de management (RJ-45 și Micro-USB) pentru configurare sistem Management in-band suportat via I/O path		
	Interfețe pentru administrare	Sistemul de stocare trebuie să ofere următoarele resurse pentru a permite administrarea echipamentului: soft management web-based GUI, soft management standalone GUI, SSH CLI, consola serial CLI, SMI-S Provider, SNMP, email, syslog alerts. Sistemul de stocare trebuie să se integreze cu softul de administrare centralizată a serverelor, permitând operațiuni de descoperire, inventariere, și monitorizare a echipamentului și să aibă minim 2 ani de suport.		
	Standarde europene	Sistemul de stocare trebuie să respecte următoarele reglementări: CE Mark (EN55032 Class A, EN55024, IEC/EN60950-1) Directiva ROHS 2011/65/EU		
	Garanție	**Minim 2 ani**, cu timp de răspuns a doua zi lucrătoare și cu remedierea defectelor la sediul clientului		
9	**Echipament de stocare a datelor pe benzi magnetice**		**buc**	**1**
	Format	Sasiu de tip montabil in cabinet metalic sau de sine stătător Dimensiune maximă 2U. Se livrează cu ansamblu de montare in cabinet metalic și echipată cu minim un cablu de alimentare de tip "10A/100-250V, C13 to IEC 320-C14 Rack Power Cable". Echipamentul ofertat se livrează cu cablu de minim 3 m de tip Mini-SAS HD la Mini-SAS HD		
	Tehnologie	Suport pentru LTO Ultrium 9		
	Interfața	Minim 2 porturi 12Gb SAS x1 ports (Mini-SAS HD SFF-8644)		
	Număr sloturi pt cartușe	minim 1		
	Capacități cartuse suportate	LTO 9: 18 TB nativ		
	Rata de transfer date	LTO 9: 300 MB/s nativ		
	Cartușe necesare	Se livrează cu minim 1 cartuș de tip minim LTO Ultrium 9. Se livrează cu minim 1 cartuș de tip Cleaning		
	Caracteristici securitate	Application Managed Encryption		
	Administrare	- 1x port ethernet 10/100/1000Mb pentru status și service		
	Alimentare electrică	Minim o sursă de alimentare de maxim 75W		
	Sisteme de operare suportate	Microsoft Windows Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES)		
	Compatibilitate software de backup	Arcserve Backup, ASG Time Navigator, CommVault Simpana, Dell/EMC NetWorker, IBM Spectrum Protect, HPE/Micro Focus Data Protector, Microsoft System Center Data Protection Manager, Veritas Backup Exec și altele.		
	Garanție	**Minim 2 ani** cu remedierea defectelor la sediul clientului, cu timp de răspuns a doua zi lucrătoare		
10	**Licenta aplicație mediu virtual**		**buc**	**2**
	Funcționalități	Licențele software ofertate vor asigura toate funcționalitățile minimale solicitate, vor fi conforme întocmai schemei de licențiere a producătorului licențelor software ofertate pentru toata puterea de calcul și de stocare a serverelor pe care aceste licențe software se instalează. Ofertantul are obligația de a detalia în oferta tehnica denumirea comercială a produsului ofertat, codul comercial al produsului ofertat, producătorul și cantitatea ofertată. Oferta tehnica ce nu conține aceste informații detaliate esențiale va fi declarată neconformă. Licențele software vor fi de tip perpetu, non-OEM, vor permite instalarea și utilizarea lor de către Beneficiar pe orice echipament de calcul funcție de cerințele de procesare și stocare viitoare.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		⍰ Să nu depindă de un sistem de operare gazdă a cărui actualizare să afecteze disponibilitatea și funcționalitatea serverelor, respectiv a mașinilor virtuale care rulează pe serverele respective; ⍰ Amprenta pe disc a hypervisor-ului să fie cât mai mică (sub 1,5 GB) astfel încât instalarea hypervisor-ului să fie făcută foarte rapid (direct pe server) chiar și din rețea, oferind totodată posibilitatea de boot-are de pe stick USB; ⍰ Suport pentru USB 3.0; ⍰ Suport pentru accelerare video hardware pentru mașinile virtuale cu sisteme de operare Linux sau Windows; ⍰ Să ofere o securitate crescută prin încărcarea proceselor importante la nivel de hypervisor în zonele de memorie reziliente, prin utilizarea ultimelor funcționalități disponibile în noile versiuni de procesoare; ⍰ Să ofere o scalabilitate crescută prin configurarea în clustere de înaltă disponibilitate; ⍰ Să dispună de capacități de failover astfel încât, în cazul defectării unui host, mașinile virtuale care rulau pe acel host să fie restartate automat pe celelalte host-uri din cluster; ⍰ Să dispună de capacități de failover astfel încât, în cazul blocării sistemului de operare instalat într-o mașină virtuală, respectiva mașină virtuală să fie restartată automat pe același host pentru deblocarea sistemului de operare, a serviciilor și aplicațiilor; ⍰ Să dispună de capacitate de failover care să detecteze problemele de acces la datastore la nivel de host și să restarteze automat mașinile virtuale afectate pe un alt host din cluster; ⍰ Să permită identificarea și evitarea situațiilor de split-brain prin monitorizarea stării host-urilor atât la nivelul rețelei de management cat și la nivelul storage-ului comun; ⍰ Să permită replicarea mașinilor virtuale la nivel de host, independent de tipul stocării folosite la sursă și destinație, asigurand un RPO (recovery point objective) de minim 5 minute; ⍰ Să permită stabilirea unei politici de retentive a replicărilor cu peste 20 de replici în timp (exemplu: 4 replici pe zi, timp de 6 zile), care vor permite refacerea sistemului replicat prin procedura de recuperare din snapshot, soluție utilă pentru refacerea în cazul coruperii datelor sau virusării; ⍰ Să ofere posibilitatea mutării simultane a mașinilor virtuale (minim 4, pe legături Gigabit/10 Gigabit) în funcționare de pe un host pe altul/altele fără afectarea funcționării acestora pentru a se putea executa activități de mentenanță pe host-ul respective; ⍰ Să asigure rate mari de consolidare a mașinilor virtuale pe host-uri prin mecanisme de optimizare și supra alocare a memoriei (ex "Memory Ballooning", "Transparent Page Sharing", "Memory Compression", "Swap to disk") pentru reducerea costurilor asociate infrastructurii fizice (exemplu: număr host-uri, număr porturi de rețea/switch-uri); ⍰ Sisteme de operare suportate pe mașinile virtuale: ⍰ Windows (Server: 2016, 2012 R2, 2008 R2, 2003 R2, Desktop: 10, 8.1, 7), Red Hat, SuSE, Ubuntu, FreeBSD, CentOS, Solaris, Oracle Linux, Mac OS X Server; ⍰ Aplicația de virtualizare să permită configurarea și rularea unor mașini virtuale cu până la 128 procesoare virtuale și 6TB RAM; ⍰ Să suporte diverse tipuri de storage (SAN, NAS, iSCSI) și protocoale de access (FC, FCOE, ISCSI, NFS) la nivel de cluster; ⍰ Suport larg din partea ISV (Independent Software Vendors) terți pentru aplicațiile Tier 1 și nu numai – exemplu: Microsoft – SQL, Exchange, SharePoint, Oracle – RAC, SAP – HANA; ⍰ Posibilitatea utilizării unui echipament de stocare extern pentru mai multe host-uri; storage-ul trebuie să poată stoca atât mașina virtuală cât și hard disk-urile virtuale asociate acesteia; ⍰ Să permită o integrare nouă și un cadru de management automatizat, bazat pe politici, pentru sistemele externe de stocare (SAN sau NAS) care să ofere un model operațional optimizat pentru mediul de lucru virtual, centrat pe nevoile aplicațiilor și nu pe infrastructură;		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		▯ Accesul către sistemul de stocare extern să poată fi făcut pe mai multe căi (multipathing), asigurându-se suport pentru failover şi load balancing, oferind şi posibilitatea de alegere a politicii de stabilire a căii de acces (exemplu: fixă, MRU, Round Robin); ▯ Sistemul de fişiere va permite accesul concurent a mai multor servere fizice (host) şi a mai multor maşini virtuale la aceeaşi resursă de stocare; ▯ Sistemul de fişiere trebuie să asigure că o maşină virtuală este accesată doar de pe un singur host (sistem de blocarea accesului); în caz de defectare a host-ului, maşina virtuală trebuie să poată fi restartată de pe alt server fizic; ▯ Sistemul de fişiere va asigura posibilitatea migrării în timp real (fără întreruperea funcţionării) unei maşini virtuale de pe un host pe altul; ▯ Sistemul de fişiere trebuie să suporte expansiunea dinamică a volumelor şi LUN-urilor la capacităţi mai mari de 2TB; ▯ Software-ul instalat pe host trebuie să poată crea echipamente de reţea virtuale (switch-uri) la care să se conecteze maşinile virtuale şi interfeţele de reţea fizice de pe host; ▯ Aplicaţia de virtualizare trebuie să permită managementul salvărilor contextuale (snap-shot) ale maşinilor virtuale fără afectarea stării de funcţionare, astfel încât o maşină virtuală se va putea restaura din orice salvare anterioară; ▯ Interfaţa unică de management bazată pe interfaţa web, accesibilă de pe browser-e Firefox (Windows, Mac OSX), Google Chrome (Windows, Mac OSX) şi IE (Windows) pentru simplificarea managementului; Soluţia de management centralizat să fie disponibilă ca appliance virtual pentru simplificarea instalării, actualizării şi administrării precum şi pentru reducerea costurilor asociate (exemplu: licenţa Windows, licenţa bază de date SQL sau Oracle).		
	Servicii de garanţie	▯ Servicii de suport şi subscripţie software pentru **minim 2 ani** cu SLA de Luni până Vineri, 12 ore pe zi. Serviciile vor asigura acces, pentru persoanele desemnate de la Beneficiar, la kiturile software de update şi upgrade ale produselor ofertate în portalul producătorului licenţelor software ofertate, precum şi acces la librăria de cunoştinţe a producătorului licenţelor ofertate pentru identificarea rapidă a soluţiilor de optimizare şi/sau de rezolvare a unor probleme de performanţă şi disponibilitate a soluţiei software de virtualizare ofertate. ▯ Pentru rezolvarea rapidă a incidentelor de garanţie ce afectează funcţionarea şi disponibilitatea soluţiei de virtualizare ofertate şi repunerea acesteia în producţie, serviciile de garanţie ofertate vor asigura servicii de suport de la distanţă de la echipele tehnice ale furnizorului. Pentru incidentele critice de severitate 1, pentru situaţiile în care soluţia de virtualizare nu este funcţională, serviciile de garanţie ofertate trebuie să asigure un timp maxim de răspuns de 4 ore.		
11	**Echipament procesare date tip 1**		**buc**	**1**
	Procesor	▯ Minim 2 procesoare suportate. ▯ Minim 2 procesoare instalate. ▯ Procesor CISC x86, minim 16 nuclee fizice, frecventa de baza minim 2.9 GHz, minim 24 MB cache pentru fiecare procesor. ▯ Suport pentru memorie minim DDR4 – 3200 Mhz ▯ Serverul trebuie să suporte instalarea a minim 2 procesoare cu cate 40 cores şi TDP 270W ▯ Minim 64x PCIe 4.0 lanes per CPU		
	Placa de bază	▯ Chipset Intel C621A sau echivalent cu suport pentru procesorul cu caracteristicile tehnice de mai sus. ▯ Pe placa de baza a serverului trebuie să apară inscriptionat numele producatorului serverului.		
	Memorie	▯ 128 GB memorie RAM tip DDR4-3200 Mhz instalata (module de minim 32 GB dual rank x4). ▯ Minim 8 canale de memorie per processor ▯ Serverul trebuie să suporte minim următoarele tipuri de protecţie a memoriei: ECC, SDDC, ADDDC si memory mirroring.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		? Serverul trebuie să suporte tehnologia de memorie persistentă, minim 16x Intel Optane Persistent Memory 200 Series modules (8 per procesor) pentru creşterea performanţelor aplicaţiilor. ? Serverul trebuie să suporte minim 32 module de memorie. ? Serverul trebuie să ofere posibilitatea de creştere a capacităţii de memorie până la minim 8TB utilizând module de memorie de tip DIMM şi până la minim 12TB utilizând module de memorie de tip DIMM (minim 4TB) şi module de memorie persistentă. ? Serverul trebuie sa suporte module RDIMM si 3DS RDIMM ? Memoriile trebuie să aibă o semnătura unică programată care să permită serverului să verifice dacă memoria este calificată şi suportată.		
	Capacitate de stocare internă instalată	Minim 8 unităţi de stocare HDD 12Gbps SAS cu capacitate de minim 2400GB la 10k rpm fiecare, de tip hot-swap. Minim 2 unităţi de stocare SSD 6Gbps SATA de tip M.2 cu capacitate de minim 240GB fiecare (minim 1.5DWPD, 67k IOPS citire, 40k IOPS scriere) instalate în RAID-1, pentru instalarea sistemului de operare.		
	Capacitate de stocare internă suportată	Serverul trebuie să dispună de minim 8 sloturi hot-swap de tip SAS/SATA. Serverul trebuie să suporte prin upgrade ulterior adăugarea a încă 16 sloturi hot-swap de tip SAS/SATA/NVME frontal. Suport pentru instalarea a minim 2 discuri M.2 sau 7 mm pentru instalare OS. Suport pentru Intel VROC NVMe RAID sau echivalent Suport pentru intermixarea în sistem a discurile SAS, SATA Suport pentru instalarea în acelaşi tip de lăcaş a discurilor de tip SAS, SATA sau U.2 NVME Serverul trebuie să suporte prin upgrade ulterior, în funcţie de tipul de unitate de stocare aleasă, o capacitate de minim: Unităţi de stocare în format 2.5": 1228.8TB prin utilizarea a 40x 30.72TB 2.5" SAS/SATA SSDs 491.52TB prin utilizarea a 32x 15.36TB 2.5" NVMe SSDs 96TB prin utilizarea a 40x 2.4TB 2.5" HDDs 1.92TB prin utilizarea a 2x 0.96TB 7mm SSDs Unităţi de stocare 3.5": 400TB prin utilizarea a 20x 20TB 3.5" HDDs 307.2TB prin utilizarea a 20x 15.36TB 3.5" SAS/SATA SSDs 153. 6TB prin utilizarea a 12x 12.8TB 3.5" NVMe SSDs		
	Controller stocare intern	Serverul trebuie să dispună de minim 12 porturi SATA onboard. Serverul trebuie să dispună de minim 12 porturi NVME onboard Serverul trebuie să dispună de un controller RAID care să suporte minim 8 unităţi de stocare SAS 12Gbps. Controller RAID cu suport pentru RAID 0, 1, 10, 5, 50, 6, 60. Suport pentru JBOD. PCIe 4.0 x8 12 Gbps SAS RAID controller Suport pentru intermixarea unităţilor de stocare SAS şi SATA (HDD şi SSD) Suport pentru intermixarea unităţilor de stocare 6Gbps şi 12Gbps Suport pentru 512e, 512n şi 4K sector formatted drives Suport pentru configurarea stripsize până la 1 MB. Suport pentru discuri virtuale mai mari de 2TB Suport pentru TRIM şi UNMAP Suport pentruAuto-resume on array rebuild (dacă se întrerupe alimentarea cu energie electrică), Online Capacity Expansion, Online RAID Level Migration, Fast initialization for quick array setup, Consistency check for background data integrity, Patrol read for media scanning and repairing, Global and dedicated hot spare, Drive roaming, SED support, Hardware Secure Boot 4GB cache cu protectie de tip flash backup. Posibilitatea administrării prin interfaţa de administrare a serverului.		
	Interfaţa video	Integrată pe placa de baza, min. 16 MB RAM dedicat, care sa suporte rezoluţie minimă 1920x1200 la 60 Hz cu 32 bits per pixel		
	Interfeţe reţea	Un adaptor de retea cu minim patru porturi 1Gbps RJ-45 folosind slot OCP cu suport pentru: - Jumbo Frames - IEEE 802.1Q VLAN support		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		- PXE Boot - iSCSI Boot - NIC Teaming - On-chip temperature monitor - IEEE 802.3az (Energy Efficient Ethernet, EEE) - IEEE 1588/802.1AS (Precision Time Protocol, PTP) - VMware NetQueue & Microsoft VMQ - Statistics for SNMP MIB II - IEEE 802.3x flow control support - IEEE 802.3ad link aggregation support - IEEE 802.3 auto-negotiation support Un adaptor de retea cu minim 2 porturi 10Gbps SFP+ folosind slot PCIe cu suport pt urmatoarele: - Interfata: PCIe 3.0 x8 - Virtualizare: NVGRE, VXLAN, Intel Virtual Technology (VT) with VMDq for virtualization, VMware NetQueue, Microsoft VMQ, SR-IOV, - TCP/IP Layer 2: RSS, LSO, TCP/UDP/IP/SCTP Checksum Offload, IPv4, IPv6, iSCSI software initiator - IEEE 802.1Q VLAN support with VLAN tag insertion - IEEE 802.3x flow control support - IEEE 802.1p Class of Service (CoS)/QoS - EEE 802.3ad Link Aggregation Control Protocol - IEEE 802.3x Full-duplex flow control Porturile SFP+ populate cu tranceivere 10Gbps optice de tip short range, transcieverele fiind de la acelaşi producător sau recomandate de producătorul echipamentului		
	Sloturi I/O	Minim 3 sloturi PCIe 4.0 din care minim 1 sloturi PCIe 4.0 x16. Suport pana la 8 sloturi PCIe. Slot dedicat pentru adaptor OCP cu interfață PCIe 4.0 x16 Serverul trebuie să suporte prin upgrade ulterior instalarea a minimum 3x double-wide GPUs		
	Unitate Optica	Suport pentru unitate optica externa de tip DVD-RW		
	Porturi	Minim 5x USB 3.1 G1 (5 Gb/s), dintre care unul intern Minim 1x USB 2.0 pentru accesarea interfeţei de management Minim 1 porturi VGA Minim 1 port GbE 10/100/1000 Mbps RJ-45 dedicat pentru administrarea sistemului. Minim 1 conector M.2 care să suporte instalarea a doua SSD-uri sau NVMe-uri într-un modul M.2 cu suport RAID-1. Suport pentru minim 1x DB-9 COM serial port.		
	Management	Sistem încorporat de monitorizare a sistemului cu modul de management de tip out-of-band cu toate functionalitatile activate şi nelimitate în timp. Oferă capabilităţi de strângere a informaţiilor despre sistem, monitorizare a stării sistemului, alertare şi notificare, configurare a setărilor de reţea, configurare a setărilor de securitate, actualizarea firmware-ului sistemului, monitorizare în timp real a consumului de energie electrică, managementul cheilor de activare, capturare şi redare a imaginilor video când sistemul porneşte şi/sau se blochează. Oferă capabilităţi pentru accesarea de la distanţă a sistemului (de pe alt sistem), instalarea de la distanţă a sistemului de operare, afişarea graficelor istorice sau în timp real a consumului de energie şi a temperaturii. De asemenea oferă capabilităţi pentru maparea unor fişiere tip imagine (ISO) de pe un sistem de la distanţă, montarea unor fişiere de tip imagine prin protocoale HTTPS/SFTP/CIFS si NFS. Permite lucrul în mod colaborativ în consolă a minim 5 utilizatori cu posibilitatea de folosire a unui chat virtual Sistemul de management va avea suport pentru interfaţa web cu suport HTML5 (fără să necesite instalare Java sau ActiveX) cât şi pentru CLi. Managementul sistemului va putea fi făcut de asemenea şi prin intermediul unei aplicaţii mobile printr-un dispozitiv mobil iOS/Android ce se poate conecta atat la portul USB 2.0 amplasată frontal pe server cât şi prin intermediul reţelei.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		Sistemul de management trebuie să asigure administrare la distanța și prin interfețe standard în industrie: - IPMI v2.0 - SNMP v3 - CIM - REST		
	Aplicație Management Convergent	Sistemul va fi livrat cu un software de management centralizat la nivelul infrastructurii de noduri de procesare, dezvoltată de producătorul serverului, care va permite funcționalități de descoperire a elementelor administrate și inventarierea lor, monitorizarea acestora, update-uri de firmware, verificări de conformitate la nivel de firmware elemente administrate, managementul configuratiilor echipamentelor din inventar (atât cele existente integrate în soluție, vezi Anexa 1.1, cât și cele noi, livrate de Ofertant), instalarea sistemelor de operare și a hypervizor-ului sistemelor de virtualizare direct pe serverele din inventar, din consola de administrare. Soluția va permite afișarea în mod vizual a elementelor din inventar. Soluția va permite inventarierea tuturor echipamentelor ofertate (serverelor și echipamentelor de stocare) sub formă de tabele de bord (dashboard). Soluția trebuie să permită managementul și administrarea elementelor de inventar fără instalarea de agenți (agentless). Conexiunea între platforma de management și echipamentele aflate sub management trebuie să fie una securizată (SSL). Managementul echipamentelor trebuie să fie unul unitar și integrat la nivelul soluției care să permită definirea de profile ce pot fi associate echipamentelor din inventar și aplicate acestora. La nivelul soluției de management trebuie să fie disponibile informații granulare asupra echipamentelor server aflate în management (configurație procesor, memorie, interfețe IO) cât și nivelul de firmware ce rulează pe acestea și sistemul de operare. Soluția de management trebuie să dispună de funcționalități de integrare în platforme de orchestrare prin intermediul REST API (standard deschis). În cadrul platformei se va regăsi posibilitatea folosirii unei interfețe de tip PowerShell care să permită rularea de script-uri. De asemenea, trebuie să permită conectori de integrare cu soluții de management al platformelor de virtualizare (VMware și Hiper-V Microsoft). Soluția propusă trebuie să dispună de mecanisme de autentificare ce permit conectarea la un server extern de tip LDAP/Active Directory. Soluția trebuie să dispună de metode vizuale de afișare a consumului de energie a mașinilor server aflate în inventar. Nodurile ofertate trebuie să fie compatibile și certificate pentru soluția software de management ofertată și să permită toate funcționalitățile de administrare ale acesteia. Softul de management trebuie să includă suport telefonic de la furnizor pe o perioada de minim 2 ani 24x7.		
	Carcasa	Rackmountable 19", maxim 2U, kit de montare în rack inclus, cu suport pentru brat de cablare.		
	Securitate	Serverul trebuie să includă modul de securitate Trusted Platform Module (TPM) 2.0. Serverul trebuie să suporte prin upgrade ulterior securizarea accesului la discuri cu panou cu cheie. Serverul trebuie să suporte prin upgrade ulterior securizarea cu un modul de alertare sau blocare a serverului în cazul în care se încearcă deschiderea carcasei.		
	Ventilatoare	Minim 6 ventilatoare 60 mm hot swap, redundante N+1, de tip single-rotor. Sursele de alimentare vor fi prevăzute cu ventilatoare integrate.		
	Surse alimentare electrică	Minim 2 surse de 1100W, clasa de eficienta Platinum, redundante, hot swap, cu cabluri de alimentare C13-C14 de minimum 2.7m.		
	Compatibilitate sisteme de operare	Serverul trebuie să fie compatibil cu minim următoarele sisteme de operare (suportate și certificate): Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi		
	Sistem de operare	Serverul trebuie să dispună de o licență Microsoft Windows Server 2022 Standard pentru toate core-urile de procesare și să fie însoțită de un kit media pentru reinstalări ulterioare.		
	Certificări	CE, EN55032 Class A, EN62368-1, EN55024, EN55035, EN61000-3-2, EN61000-3-3, (EU) 2019/424 si EN50581		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		Energy Star 3.0		
	Garanție	**Minim 2 ani**, cu timp de răspuns a doua zi lucrătoare și cu remedierea defectelor la sediul clientului		
12	**Echipament procesare date tip 2**		**buc**	**1**
	Procesor	Minim 2 procesoare suportate. Minim 1 procesor instalat. Procesor CISC x86, minim 10 nuclee fizice, frecvența de bază minim 2.3 GHz, minim 15 MB cache pentru fiecare procesor. Suport pentru memorie minim DDR4 – 2667 Mhz Serverul trebuie să suporte instalarea a minim 2 procesoare cu cate 40 core-uri și TDP 270W Minim 64x PCIe 4.0 lanes per CPU		
	Placa de baza	Chipset Intel C621A sau echivalent cu suport pentru procesorul cu caracteristicile tehnice de mai sus. Pe placa de baza a serverului trebuie să apară inscriptionat numele producătorului serverului.		
	Memorie	64 GB memorie RAM tip DDR4-3200 Mhz instalata (module de minim 32 GB dual rank x4). Minim 8 canale de memorie per processor. Serverul trebuie să suporte minim următoarele tipuri de protecție a memoriei: ECC, SDDC, ADDDC și memory mirroring. Serverul trebuie să suporte tehnologia de memorie persistentă, minim 16x Intel Optane Persistent Memory 200 Series modules (8 per procesor) pentru creșterea performanțelor aplicațiilor. Serverul trebuie să suporte minim 32 module de memorie. Serverul trebuie să ofere posibilitatea de creștere a capacității de memorie pana la minim 8TB utilizând module de memorie de tip DIMM și până la minim 12TB utilizând module de memorie de tip DIMM (minim 4TB) și module de memorie persistentă. Serverul trebuie să suporte module RDIMM și 3DS RDIMM Memoriile trebuie să aibă o semnătura unică programată care să permită serverului să verifice dacă memoria este calificată și suportată.		
	Capacitate de stocare internă instalată	Minim 8 unități de stocare HDD 12Gbps SAS cu capacitate de minim 2400GB la 10k rpm fiecare, de tip hot-swap.		
	Capacitate de stocare internă suportată	Serverul trebuie să dispună de minim 24 sloturi hot-swap de tip SAS/SATA amplasate frontal. Suport pentru instalarea a minim 2 discuri M.2 sau 7 mm pentru instalare OS. Suport pentru Intel VROC NVMe RAID sau echivalent Suport pentru intermixarea în sistem a discurile SAS, SATA Suport pentru instalarea în același tip de lăcaș a discurilor de tip SAS, SATA sau U.2 NVME Serverul trebuie să suporte prin upgrade ulterior, în funcție de tipul de unitate de stocare aleasă, o capacitate de minim: Unități de stocare în format 2.5": 1228.8TB prin utilizarea a 40x 30.72TB 2.5" SAS/SATA SSDs 491.52TB prin utilizarea a 32x 15.36TB 2.5" NVMe SSDs 96TB prin utilizarea a 40x 2.4TB 2.5" HDDs 1.92TB prin utilizarea a 2x 0.96TB 7mm SSDs Unități de stocare 3.5": 400TB prin utilizarea a 20x 20TB 3.5" HDDs 307.2TB prin utilizarea a 20x 15.36TB 3.5" SAS/SATA SSDs 153. 6TB prin utilizarea a 12x 12.8TB 3.5" NVMe SSDs		
	Controller stocare intern	Serverul trebuie să dispună de minim 12 porturi SATA onboard. Serverul trebuie să dispună de minim 12 porturi NVME onboard		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		Serverul trebuie să dispună de un controller RAID care să suporte minim 32 unități de stocare SAS 12Gbps. Controller RAID cu suport pentru RAID 0, 1, 10, 5, 50, 6, 60. Suport pentru JBOD. PCIe 4.0 x8 12 Gbps SAS RAID controller Suport pentru intermixarea unităților de stocare SAS și SATA (HDD și SSD) Suport pentru intermixarea unităților de stocare 6Gbps și 12Gbps Suport pentru 512e, 512n și 4K sector formatted drives Suport pentru configurarea stripsize până la 1 MB. Suport pentru discuri virtuale mai mari de 2TB Suport pentru TRIM și UNMAP Suport pentruAuto-resume on array rebuild (dacă se întrerupe alimentarea cu energie electrică), Online Capacity Expansion, Online RAID Level Migration, Fast initialization for quick array setup, Consistency check for background data integrity, Patrol read for media scanning and repairing, Global and dedicated hot spare, Drive roaming, SED support, Hardware Secure Boot 8GB cache cu protectie de tip flash backup. Posibilitatea administrării prin interfața de administrare a serverului.		
	Interfața video	Integrată pe placa de baza, min. 16 MB RAM dedicat, care sa suporte rezoluție minima 1920x1200 la 60 Hz cu 32 bits per pixel		
	Interfețe rețea	Un adaptor de retea cu minim patru porturi 1Gbps RJ-45 folosind slot OCP cu suport pentru: - Jumbo Frames - IEEE 802.1Q VLAN support - PXE Boot - iSCSI Boot - NIC Teaming - On-chip temperature monitor - IEEE 802.3az (Energy Efficient Ethernet, EEE) - IEEE 1588/802.1AS (Precision Time Protocol, PTP) - VMware NetQueue & Microsoft VMQ - Statistics for SNMP MIB II - IEEE 802.3x flow control support - IEEE 802.3ad link aggregation support - IEEE 802.3 auto-negotiation support Un adaptor de retea cu minim 2 porturi 10Gbps SFP+ folosind slot PCIe cu suport pt urmatoarele: - Interfata: PCIe 3.0 x8 - Virtualizare: NVGRE, VXLAN, Intel Virtual Technology (VT) with VMDq for virtualization, VMware NetQueue, Microsoft VMQ, SR-IOV, - TCP/IP Layer 2: RSS, LSO, TCP/UDP/IP/SCTP Checksum Offload, IPv4, IPv6, iSCSI software initiator - IEEE 802.1Q VLAN support with VLAN tag insertion - IEEE 802.3x flow control support - IEEE 802.1p Class of Service (CoS)/QoS - EEE 802.3ad Link Aggregation Control Protocol - IEEE 802.3x Full-duplex flow control Porturile SFP+ populate cu tranceivere 10Gbps optice de tip short range, transcieverele fiind de la același producător sau recomandate de producătorul echipamentului		
	Alte interfețe	Adaptor extern de tip SAS: • PCIe 3.0 x8 host interface • 12Gbps SAS/SATA (suporta 3/6Gbps SATA si 3/6/12Gbps SAS) • Minim 2 porturi externe SFF-8644 • Suporta conectarea unităților de stocare externe și a unităților de bandă		
	Sloturi I/O	Minim 3 sloturi PCIe 4.0 din care minim 1 sloturi PCIe 4.0 x16. Suport pana la 8 sloturi PCIe. Slot dedicat pentru adaptor OCP cu interfață PCIe 4.0 x16 Serverul trebuie sa suporte prin upgrade ulterior instalarea a minim 3x double-wide GPUs		
	Unitate Optica	Suport pentru unitate optica externa de tip DVD-RW		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
	Porturi	Minim 5x USB 3.1 G1 (5 Gb/s), dintre care unul intern Minim 1x USB 2.0 pentru accesarea interfeței de management Minim 1 porturi VGA Minim 1 port GbE 10/100/1000 Mbps RJ-45 dedicat pentru administrarea sistemului. Minim 1 conector M.2 care sa suporte instalarea a doua SSD-uri sau NVMe-uri intr-un modul M.2 cu suport RAID-1. Suport pentru minim 1x DB-9 COM serial port.		
	Management	Sistem încorporat de monitorizare a sistemului cu modul de management de tip out-of-band cu toate funcționalitățile activate și nelimitate în timp. Oferă capabilități de strângere a informațiilor despre sistem, monitorizare a stării sistemului, alertare și notificare, configurare a setărilor de rețea, configurare a setărilor de securitate, actualizarea firmware-ului sistemului, monitorizare în timp real a consumului de energie electrică, managementul cheilor de activare, capturare și redare a imaginilor video cand sistemul pornește și/sau se blochează. Oferă capabilități pentru accesarea de la distanță a sistemului (de pe alt sistem), instalarea de la distanță a sistemului de operare, afișarea graficelor istorice sau în timp real a consumului de energie și a temperaturii. De asemenea oferă capabilități pentru maparea unor fișiere tip imagine (ISO) de pe un sistem de la distanță, montarea unor fișiere de tip imagine prin protocoale HTTPS/SFTP/CIFS si NFS. Permite lucrul în mod colaborativ în consola a minim 5 utilizatori cu posibilitatea de folosire a unui chat virtual. Sistemul de management va avea suport pentru interfața web cu suport HTML5 (fără să necesite instalare Java sau ActiveX) cât și pentru CLi. Managementul sistemului va putea fi făcut de asemenea și prin intermediul unei aplicații mobile printr-un dispozitiv mobil iOS/Android ce se poate conecta atât la portul USB 2.0 amplasată frontal pe server cât și prin intermediul rețelei. Sistemul de management trebuie să asigure administrare la distanță și prin interfețe standard în industrie: - IPMI v2.0 - SNMP v3 - CIM - REST		
	Aplicație Management Convergent	Sistemul va fi livrat cu un software de management centralizat la nivelul infrastructurii de noduri de procesare, dezvoltată de producătorul serverului, care va permite funcționalități de descoperire a elementelor administrate și inventarierea lor, monitorizarea acestora, update-uri de firmware, verificări de conformitate la nivel de firmware elemente administrate, managementul configurațiilor echipamentelor din inventar (atât cele existente integrate în soluție, vezi Anexa 1.1, cât și cele noi, livrate de Ofertant), instalarea sistemelor de operare și a hypervizor-ului sistemelor de virtualizare direct pe serverele din inventar, din consola de administrare. Soluția va permite afișarea în mod vizual a elementelor din inventar. Soluția va permite inventarierea tuturor echipamentelor ofertate (serverelor și echipamentelor de stocare) sub forma de tabele de bord (dashboard). Soluția trebuie să permită managementul și administrarea elementelor de inventar fără instalarea de agenți (agentless). Conexiunea între platforma de management și echipamentele aflate sub management trebuie să fie una securizată (SSL). Managementul echipamentelor trebuie să fie unul unitar și integrat la nivelul soluției care să permită definirea de profile ce pot fi associate echipamentelor din inventar și aplicate acestora. La nivelul soluției de management trebuie să fie disponibile informații granulare asupra echipamentelor server aflate în management (configurație procesor, memorie, interfețe IO) cât și nivelul de firmware ce rulează pe acestea și sistemul de operare. Soluția de management trebuie să dispună de funcționalități de integrare în platforme de orchestrare prin intermediul REST API (standard deschis). În cadrul platformei se va regăsi posibilitatea folosirii unei interfețe de tip PowerShell care să permită rulea de script-uri. De asemenea, trebuie să permită conectori de integrare cu soluții de management al platformelor de virtualizare (VMware și Microsoft). Soluția		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		propusă trebuie să dispună de mecanisme de autentificare ce permit conectarea la un server extern de tip LDAP/Active Directory. Soluția trebuie să dispună de metode vizuale de afișare a consumului de energie a mașinilor server aflate în inventar. Nodurile ofertate trebuie să fie compatibile și certificate pentru soluția software de management ofertată și să permită toate funcționalitățile de administrare ale acesteia. Softul de management trebuie să includă suport telefonic de la furnizor pe o perioada de minim 2 ani 24x7.		
	Carcasa	Rackmountable 19", maxim 2U, kit de montare în rack inclus, cu suport pentru brat de cablare.		
	Securitate	Serverul trebuie să includă modul de securitate Trusted Platform Module (TPM) 2.0. Serverul trebuie să suporte prin upgrade ulterior securizarea accesului la discuri cu panou cu cheie. Serverul trebuie să suporte prin upgrade ulterior securizarea cu un modul de alertare sau blocare a serverului în cazul în care se încearcă deschiderea carcasei.		
	Ventilatoare	Minim 6 ventilatoare 60 mm hot swap, redundante N+1, de tip single-rotor. Sursele de alimentare vor fi prevăzute cu ventilatoare integrate.		
	Surse alimentare electrică	Minim 2 surse de 750W, clasa de eficienta Platinum, redundante, hot swap, cu cabluri de alimentare C13-C14 de minimum 2.7m.		
	Compatibilitate sisteme de operare	Serverul trebuie să compatibil cu minim următoarele sisteme de operare (suportate și certificate): Microsoft Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, VMware ESXi		
	Sistem de operare	Serverul trebuie sa dispuna de o licenta Microsoft Windows Server 2022 Standard pentru toate core-urile de procesare și să fie însoțită de un kit media pentru reinstalari ulterioare.		
	Certificări	CE, EN55032 Class A, EN62368-1, EN55024, EN55035, EN61000-3-2, EN61000-3-3, (EU) 2019/424 si EN50581 Energy Star 3.0		
	Garanție	**Minim 2 ani**, cu timp de răspuns a doua zi lucrătoare și cu remedierea defectelor la sediul clientului		
13	**Echipament tip UPS**		**buc**	**4**
	Format	3 unități de rack Instalabil în cabinet metalic standard și/sau instalabil sub forma de turn de sine stătător		
	Topologie	Online, dubla conversie, ieșire sinusoidală		
	Putere	Minim 5000VA / 4500W		
	Caracteristici electrice de intrare	Voltaj: 200-240V AC Frecventa: 50/60 Hz Amperaj maxim: 25A		
	Caracteristici electrice de ieșire	Voltaj: 200/208/220/230/240 V AC Frecventa: 50/60 Hz Putere de iesire: 200-240 V AC: 5000 VA/4500W Conectori iesire: - Minim 2x IEC 320-C19 (16A) Minim 8x IEC 320-C13 (10A)		
	Baterii	Tip VRLA; Nu necesita mentenanta; Sigilate și etanșe Management: test automat al bateriilor și protectie la descărcare, recunoaștere automată a unităților de baterii externe Baterii de tip hot-swap Suport pentru minim 4 module externe de baterii Minim un modul extern de baterii în configurația ofertată.		
	Altele	Echipamentul ofertat trebuie sa fie însoțit de cablu de alimentare de la rețea de minim 4m, 32A, 230V, IEC 309 P+N+G.		
	Comunicații și administrare	Port USB Port Serial RS-232 (RJ-45) Port de retea 10/100 Mb (RJ-45)		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		Sistem de monitorizare a mediului de instalare: - Monitorizare minim temperatura ambientala și umiditate relativă - Suportă alarme predefinite - Posibilitate trimitere notificari pe email via SMTP Afișaj electronic LCD cu butoane Indicatori de tip LED Posibilitate de pornire și oprire de la distanță		
	Garanție	**Minim 2 ani**		
14	**Licenta aplicație backup date**		**buc**	**1**
	Cerințe generale	Soluția oferită trebuie sa protejeze datele prin mecanisme de copiere (backup, replicare asincrona și continua)		
		Soluția trebuie sa ofere interfețe de administrare pentru administratori atat grafic (GUI) cât și linie de comandă (CLI)		
		Soluția ofertată trebuie să fie prezentă în Gartner Magic Quadrant pentru soluții de protecție (Data Center Backup and Reocvery Solutions) și să fie prezentă în lista de referințe Gartner https://www.gartner.com/reviews/market/data-center-backup-and-recovery-solutions cu minim 100 refererințe și scor minim de 4,5.		
		Soluția propusă trebuie sa fie capabilă sa protejeze aplicația de virtualiza propusă de Ofertant.		
		Soluția trebuie să aibă mecanisme de eficiență integrată, prin care se realizează stocarea datelor, prin compresie și deduplicare. Deduplicarea trebuie să aibă opțiunea de a utiliza blocuri de 1MB sau mai mici, sau lungime variabilă.		
		Tot din considerente de eficienta, solutia oferita trebuie sa permita crearea backup-urilor incrementale și sintetice (synthetic full). Este obligatoriu ca backup-urile sintetice sa necesite timp minim de realizare, prin mecanisme de offloading către echipamentele de backup utilizate. Toate opțiunile de restaurare trebuie sa nu fie condiționate de tipul backup-urilor (incremental, sintetic, etc)		
		Soluția va avea mecanisme de criptare (standardul AES 256 sau superior). Criptarea se va realiza la sursa, și va fi utilizată atât în tranzit și cât timp datele sunt stocate. Toate opțiunile de restaurare trebuie să fie permise din backup-uri cu sau fără criptare, iar prezența criptării nu va limita operațiile de restaurare.		
		Soluția propusă trebuie sa ofere inamovibilitatea datelor (mecanisme de garantare a datelor la scriere și ștergere). Dacă soluția va fi oferită cu hardware, funcțiile de inamovibilitate trebuie să fie incluse.		
		Soluția propusă trebuie să protejeze 30 mașini virtuale, indiferent de modalitatea de licențiere a producătorului.		
		Soluția propusă trebuie sa includa minim 2 ani de suport de la furnizor.		
	Functionalitati specifice pentru Optimizarea costurilor	Soluția oferită trebuie să implementeze toate componentele (data mover, proxies, noduri de criptare, etc) că virtual și/sau fizice. Dacă sunt necesare noduri fizice pentru a satisface prezentele cerințe, sau în cazul în care solutia ofertata nu satisface prezentele cerințe și este nevoie de un echipament specializat de stocare, acestea trebuie incluse în prezenta ofertă.		
		Soluția oferită va include software și platforma hardware de stocare a backupurilor.		
		Pentru apliance-urile hardware și soluțiile cu hardware specific, toate functionalitatile cerute vor fi incluse și licentiate pe respectivele echipamente.		
		Soluțiile software vor demonstra integrarea cu cel puțin 3 echipamente de backup, dintre următoarele: DataDomain (cu protocolul DDBoost), HPE StoreOnce (cu protocolul Catalyst), Quantum Dxi, CleverSafe, Exagrid, Windows ReFS si Linux XFS.		
		Soluțiile hardware sau soluțiile tip appliance vor fi oferite în configurații No-Single-Point of Failure.		
		Soluțiile software vor trebui sa ofere rezilienta catalogului pentru metadate, astfel incat datele din backup sau replicile să poată fi utilizate în cazul defectărilor hardware și a pierderii cataloagelor interne.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		Soluția propusă trebuie să poată virtualiza storage-ul de backup, prin unificarea mai multor spații de stocare de pe unul sau mai multe echipamente hardware, oferind capacitate nelimitată de stocare. Storage-ul virtual trebuie să permită mutarea backup-urilor și să elibereze capacități de stocare pentru upgrade-uri ale echipamentelor sau alte operații administrative, fără impact în operațiile de back-up și restaurare.		
		Soluția oferită trebuie să implementeze toate componentele (data mover, proxies, noduri de criptare, etc) că virtual și/sau fizice. Dacă sunt necesare noduri fizice pentru a satisface prezentele cerințe, sau în cazul în care soluția ofertată nu satisface prezentele cerințe și este nevoie de un echipament specializat de stocare, acestea trebuie incluse în prezenta oferta.		
	Functionalitati specifice pentru cantitatea maximă acceptabilă de pierderi de date măsurată în timp și durata necesară pentru a se recupera acestora în cazul unui incident	Solutia ofertata trebuie sa permita realizarea backup-urilor consistente pentru aplicații, inclusiv pentru baze de date Oracle, Microsoft SQL, PostgreSQL si MySQL.		
		Soluția oferită trebuie să permită recuperarea granulară a fișierelor sau folderelor, prin extragerea lor din backup.		
		Din motive de securitate, mașinile virtualizate cu rol de baze de date nu permit instalarea de software sau agenți pentru operațiile de backup sau recuperare. Soluția ofertată trebuie să permită backupul și recuperarea datelor fără a fi nevoie de a instala software. Operațiile de restaurare granulară pentru fișiere și aplicații (inclusiv Oracle și SQL) trebuie să se realizeze direct, fără instrumente adiționale, agenți sau software ce se instalează pe aceste mașini.		
		Soluția va oferi posibilitatea utilizatorilor să utilizeze un portal cu autoservire, pentru datele pe care doresc sa le recupereze și au permisiunea administratorilor. În protalul de autoservire, administratorii trebuie să poată delega restaurările de fișiere, aplicații, baze de date (SQL, Oracle), e-mailuri și mașini virtuale.		
		Soluția oferită trebuie sa permita recuperari ultra rapide, prin pornirea imediată a acestora din backup, fara a fi necesara copierea datelor. Copierea datelor se va face după repararea mașinilor virtuale și se va face în background.		
		Recuperarea ultra rapidă trebuie sa fie disponibilă din orice backup, din orice masina (Vmware, Hyper-V, masini fizice) și sa permita recuperarea inclusiv pe o alta platforma (prin mecanisme de conversie a formatului), inclusiv operații P2V (Physical-to-virtual), V2V (Hyper-V to Vmware, Vmware to Hyper-V) și C2V (AWS to Vmware, AWS to Hyper-V, Azure to Vmware)		
		Soluția oferită trebuie să includă mecanisme de recuperare ultra rapidă pentru baze de date Oracle si Microsoft SQL, prin pornirea acestor baze din backup. Timpul de pronire al acestor baze (RTO) trebuie să fie sub 10 minute, indiferent de dimensiunea bazei.		
		Soluția oferită trebuie să ofere posibilitatea integrării cu echipamente de stocare și să poată utiliza snapshoturile acestor echipamente, atat în procesul de backup cât și dacă este necesar pentru recuperarea datelor din snapshot. Soluția ofertată trebuie să includă minim 5 vendori cu care să aibă integrare, dintre următorii: HPE, IBM, Dell-EMC, NetApp, PureStorage, Hitachi, Lenovo, Fujitsu, Huawei.		
		Soluția va avea posibilitatea setarii parametrilor pentru resursele utilizabile în procesul de backup, pentru a minimiza impactul pe mediile de producție. Astfel, soluția va prezenta capabilitatea setarilor pentru a limita banda utilizabilă în rețea, iar pentru echipamentele de stocare va putea stabili praguri la care procesele de backup vor fi oprite în cazul utilizarii intensive.		
	Funcționalități pentru reducerea riscurilor	Soluția oferită trebuie să aibă capabilitățile de a stoca backup-urile pe medii inamovibile (protejate la scriere și ștergere) cât și offline. Componentele necesare trebuie să fie incluse în ofertă dacă acestea sunt necesare (de exemplu în cazul unor echipamente specifice cu care soluția poate oferi aceste capabilități).		
		Din rațiuni de securitate, operațiile de restaurare trebuie sa permita restaurarea cu opțiunea de scanare de securitate. Operațiile de scanare trebuie sa fie incluse implicit sau să fie implementate prin operații de scripting, iar acestea trebuie sa fie incluse în ofertă.		
		Soluția oferită trebuie să includă mecanisme de testare automată a recuperarii datelor, implementate pe baza recuperărilor ultra rapide, pentru Vmware si Hyper-V. Operațiile de testare trebuie să includă pașii de recuperare, pașii de		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		verificare a aplicațiilor și bazelor de date și raportările vor include data și ora efectuării. Testarea se va efectua automat, la o data aleasa de administratori, din cel puțin o copie realizata (backup sau replică)		
		Soluția trebuie să permită recuperarea datelor din snapshoturile echipamentelor de stocare, inclusiv pentru mașini virtuale, baze de date Oracle si Microsoft SQL. Fisierele, folderele, mașinile virtuale și bazele de date, trebuie să poată fi restaurate din snapshoturile echipamentelor de stocare, indiferent de modul de creare a acestor snapshoturi (realizate de soluția ofertată sau existente pe echipament).		
		Soluția va putea realiza testarea periodică prin recuperarea automată în medii de test a datelor. Jurnalul testelor va putea fi exportat și utilizat în scopuri de raportare și audit.		
		Testarea va realiza pornirea mașinilor virtuale din backup și va realiza teste de aplicații (Active Directory, baze de date MS SQL si Oracle, servere de e-mail și servere web), incluzand rezultatul acestora în rapoartele generate.		
		Soluția va permite raportarea operațiunilor de backup, situația mașinilor protejate, capacitatea de stocare utilizata, testele de recuperare efectuate și operațiile de verificare efectuate pentru aplicații.		
	Alte cerințe specifice	Soluția va permite raportarea operațiunilor de backup, situația mașinilor protejate, capacitatea de stocare utilizată, testele de recuperare efectuate și operațiile de verificare efectuate pentru aplicații;		
		Soluția trebuie să permită generarea rapoartelor și trimiterea lor via e-mail;		
		Soluția trebuie să aibă posibilitatea de a urmări schimbările intervenite în configurația mediilor virtuale, cu posibilitatea identificării acestor modificări și a utilizatorilor care au realizat aceste schimbări;		
		Soluția trebuie să permită generarea de rapoarte pentru o perioada de timp aleasă. Intervalul de timp va putea fi ușor modificat;		
		Soluția trebuie să aibă rapoarte predefinite și să permită modificarea acestora;		
		Soluția trebuie să permită analiza obiectelor supradimensionate (mașini virtuale ce au alocate mai multe resurse decât este necesar) și va sugera o metodă de optimizare a resurselor acestora;		
		Soluția trebuie să permită generarea de rapoarte pentru modul de funcționare a soluției de protecție a datelor.		
	Garanție	Garanție și suport pentru **Minim 2 ani**		
15	**Licențe antivirus**		**buc**	**530**
	CARACTERISTICI GENERALE ALE PRODUSULUI	Produsul („soluția") reprezintă o platformă integrată pentru managementul securității, gândită ca o soluție modulară. Produsul conține următoarele module: A. O consolă de management care asigură funcționalități de administrare. B. Protecție antimalware pentru stații fizice/virtuale, laptopuri și servere C. Protecție și securitate pentru serverele email Microsoft Exchange		
	A. CONSOLA DE MANAGEMENT	A. Instalare și configurare: 1. Pachetul de instalare va fi livrat ca o mașină virtuală bazată pe un sistem de operare securizat care conține toate rolurile sau serviciile necesare. Consola nu va necesita o licență suplimentară pentru sistemul de operare. Imaginea de tip template se va putea importa în: a. VMware vSphere, View, Horizon b. Citrix XenServer, XenApp, Xen Desktop c. Microsoft Hyper-V d. Red Hat Enterprise Virtualization e. KVM sau „Kernel-based Virtual Machine" f. Oracle VM. g. Nutanix h. Alte platforme de virtualizare, la cerere 2. Consola de management se livrează cu o baza de date inclusă care este de tip non-relațională, pentru o funcționare cât mai rapidă, fără a fi nevoie de licențe adiționale. 3. Soluția va fi scalabilă, astfel ca oricare dintre roluri sau servicii pot fi instalate separat pe mai multe mașini virtuale sau pe aceeași mașină virtuală.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		4. Rolurile principale trebuie să fie cel puțin similare cu: Server cu baza de date, Server de comunicatie, Server de actualizare, Server de Web. 5. Soluția va include adițional 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 performanța/redundantă). 6. Soluția va include un mecanism de configurare a disponibilității pentru Serverul cu baze de date (clustering pentru redundanta). Astfel, baza de date se va putea instala de mai multe ori, pe mai multe mașini virtuale. 7. Mașinile de scanare pentru mediile virtuale VMware si Citrix se instalează la distanță prin task din consola de management, iar pentru alte platforme se descarcă separat din interfața web a produsului. B. Cerințe generale: 1. Interfața consolei de management va fi în limba română. 2. Interfața clientului de securitate, care se instalează pe stații și servere, va fi în limba română. 3. Manualul de instalare a produsului va fi în limba română. 4. Manualul de administrare a produsului va fi în limba română. 5. Produsul suportă licențierea per procesor fizic (socket). În felul acesta numărul mașinilor virtuale poate varia oricand, ele fiind protejate. 6. Soluția va include un modul de update server prin care se asigura actualizarea de produs și a semnăturilor. 7. Soluția va permite activarea/dezactivarea actualizarilor de produs/semnături. 8. 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. 9. Pentru o mai bună urmărire a actualizărilor consolei de management, soluția permite vizualizarea unui jurnal de modificări în care sunt precizate istoric: a. versiunea consolei de management b. data versiunii c. funcții noi și îmbunătățiri d. probleme rezolvate e. probleme cunoscute 10. Notificările – prezente în interfață, notificarile necitite sunt evidentiate, trimise către una sau mai multe adrese de email, alertează administratorul în cazul unor probleme majore: licențiere, detecție viruși, actualizări de produs disponibile). 11. Soluția va permite integrarea cu un server Syslog pentru raportarea evenimentelor antimalware. 12. Soluția va permite instalarea serviciului de SNMP prin care se pot raporta statusul mașinilor din cadrul componentei de management. 13. Soluția permite creare 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. C. Panou de monitorizare și raportare (Dashboard): 1. Rapoartele din panoul de monitorizare vor putea fi configurate specificând numele raportului, tipul raportului, ținta raportului, opțiuni specifice pentru orice tip de raport (de exemplu pentru raportul de actualizare - care este intervalul după care o stație este considerată neactualizată). 2. Panoul central conține rapoarte pentru toate modulele suportate. 3. Rapoartele din panoul central de comandă permit: adăugarea altor rapoarte, ștergerea lor și rearanjarea. D. Inventarierea rețelei – managementul securității:		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		1. Soluția se va integra cu domenii Active Directory multiple, VMware vCenter Server, Citrix Xen Server, Nutanix Prism și importa inventarul acestor platforme. 2. Se permite descoperirea stațiilor fizice neintegrate în Active Directory (Workgroup) cu ajutorul Network discovery. 3. Soluția va oferi opțiuni de căutare, sortare și filtrare după numele sistemului, sistem de operare, adresa IP, politică aplicată, ultima data când s-a conectat (online și/sau offline) și FQDN. 4. Soluția va 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 rulează sistemul de operare Windows, Linux, Mac. 5. Soluția va permite instalarea la distanță sau manual a clienților antimalware pe mașini fizice/virtuale. 6. Soluția va permite selectarea modulelor componente atunci când se creaza pachetul clientului care se instalează pe mașinile fizice/virtuale. 7. Soluția va permite lansarea de task-uri de scanare, actualizare, instalare, dezinstalarea la distanță pentru clientul antimalware. 8. Soluția va oferi posibilitatea de repornire a mașinilor fizice de la distanță. 9. Soluția va oferi informații detaliate despre fiecare task și se afișează dacă task-ul s-a finalizat sau nu cu succes. 10. Soluția va permite configurarea centralizată a clienților antimalware prin intermediul politicilor 11. Se vor oferi în consola de management informații detaliate ale obiectelor din consolă: Nume, IP, Sistem de operare, Grup, Politica atribuită, Ultimele actualizare, Versiunea produsului, Versiunea de semnături. 12. Pentru integrarea cu Active Directory, se va putea defini și intervalul (în ore) de sincronizare și forța sincronizarea. 13. Se permite descoperirea mașinilor din Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM. 14. Soluția permite descoperirea tuturor aplicațiilor instalate pe toate stațiile și serverele din rețea, prin rularea unui task din consola de administrare. E.Politici: 1. Soluția va permite configurarea setărilor clientului antimalware prin intermediul unei singure politici ce conține setări pentru toate module 2. Politica va conține opțiuni specifice de activare/dezactivare și configurarea funcționalităților precum scanarea antimalware la cerere, firewall, controlul accesului la Internet, scanarea traficului web,controlul dispozitivelor, power user, sandbox în cloud, modul avansat bazat pe tehnologii de tip machine-learning tunabil, modul de tip Endpoint-Detection and Response (EDR). 3. Soluția permite aplicarea politicilor pe mașini client, grupuri de masini, domeniu, unități organizaționale. 4. Politica sa poate fi schimbata automat în funcție de: a. IP sau clasa de IP al stației b. Gateway-ul alocat c. DNS serverul alocat d. WINS serverul alocat e. Sufix DNS pentru conexiunea dhcp f. Clientul este/nu este în aceeași rețea cu infrastructura de management (stația de lucru poate soluționa implicit numele gazdei) g. Tipul rețelei (lan, wireless) h. User-ul logat pe stație 5. Etichete definite pe mașinii virtuale în cloud (disponibile doar prin integrare Amazon EC2 sau MS Azure) F.Rapoarte: 1. Soluția va conține rapoarte care prezintă statusul mașinilor clienților din punct de vedere al actualizărilor, fișierelor malware detectate, aplicațiile blocate, site-urilor web blocate.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		2. Rapoartele programate pot fi trimise către un număr nelimitat de adrese de email (nu este nevoie să aibă un cont în consola de management). 3. Soluția va permite vizualizarea rapoartelor curente programate de administrator. 4. Soluția va permite exportarea rapoartelor în format .pdf și detaliile ca format .csv. 5. Soluția va permite filtrarea informațiilor conținute în rapoartele trimise pe mail astfel încât doar informațiile relevante cerute de către administrator vor fi transmise pe email. 6. Soluția va permite arhivarea rapoartelor care se trimit pe email. 7. Soluția include un generator de rapoarte care oferă posibilitatea de a investiga o problema de securitate pe baza mai multor criterii, menținând informațiile concise și ordonate corespunzător. Astfel, soluția include interogări precum: starea terminalului, evenimente terminal, evenimente Exchange. 8. Interogarea legată de starea terminalului include informații precum: a. tip mașină b. infrastructura rețelei căreia îi aparține terminalul c. datele agentului de securitate d. starea modulelor de protectie e. rolurile terminalelor. 9. Interogarea legată de evenimente terminal include informații precum: a. calculatorul țintă pe care a avut loc evenimentul b. tipul starea și configurația agentului de securitate instalat c. starea modulelor și rolurilor de protectie instalate pe agentul de securitate d. denumirea și alocarea politicii e. utilizatorul autentificat în timpul evenimentului f. evenimente (site-uri blocate, aplicații blocate, detecțiile etc) 10. Interogarea legată de evenimente Exchange include informații precum: a. Direcția traficului e-mail b. Evenimente de securitate (detectarea programelor de tip malware sau a fișierelor atașate) c. Măsurile implementate în fiecare situație (curățarea, ștergerea, înlocuirea sau carantinarea fișierului, ștergerea sau respingerea e-mail-ului) G. Carantina: 1. Soluția va permite restaurarea fișierelor carantinate în locația originală sau într-o cale configurabilă. 2. Carantina va fi locală, pe fiecare stația administrată și va fi administrată, fie local, fie din consola de management. 3. Permite descărcarea fișierelor carantinate doar pentru mașinile virtuale protejate prin modulul mediilor virtuale integrat cu aplicația de virtualizare ofertată de Ofertant H. Utilizatori: 1. Administrarea se va putea face pe baza de roluri. 2. Roluri multiple predefinite: Administrator companie, Administrator retea, Reporter sau rol personalizat. a. Administrator companie: administrează arhitectura consolei de management; b. Administrator rețea: administrează serviciile de securitate; c. Reporter: monitorizează și genereaza rapoarte. 3. Utilizatorii pot fi importați din Microsoft Active Directory sau creați în consola de management. 4. Se va permite configurarea detaliată a drepturilor administrative, permițând selectarea serviciilor și obiectelor pentru care un utilizator poate face modificări. 5. Se va permite deconectarea automată a oricărui tip de utilizator după un anumit timp pentru o protecție sporită a datelor afișate în consola de administrare. Acest interval se poate personaliza de administratorul soluției. I. Log-uri:		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		1. Înregistrarea acțiunilor utilizatorilor. 2. Se vor oferi informații detaliate pentru fiecare acțiune a unui utilizator. 3. Se va permite filtrarea acțiunilor utilizator după numele utilizatorului, acțiune. J. Actualizare: 1. Se permite definirea de locații de actualizare multiple. 2. Se permite activarea/dezactivarea actualizarilor de produs și semnături. 3. Se permite actualizarea produsului într-o rețea fără acces la Internet. 4. Orice client antivirus să poată fi configurat să livreze update-urile către alt client antivirus 5. Soluția dispune un server de actualizare (update) care face posibilă stabilirea componentelor ce vor fi descărcate automat de pe internet, fără intervenția administratorului. Astfel, administratorul va putea descărca pachetele pentru protecția stațiilor și serverelor pe care rulează sistemul de operare Windows, Linux, Mac sau, poate descărca pachetele pentru modul de scanare centralizată în mediile de virtualizare VMware, Hyper-V sau Citrix. 6. În cadrul serverului de actualizare, pentru o mai bună urmărire a actualizărilor pachetele pentru protecția stațiilor și serverelor sau a pachetelor pentru modul de scanare centralizată, se va putea vizualiza un jurnal de modificări în care sunt precizate istoric: a. versiunea pachetului b. data versiunii c. funcții noi și îmbunătățiri d. probleme rezolvate e. probleme cunoscute 7. Soluția permite testarea noilor versiuni de pachete de instalare ale clientului antimalware, înainte de a fi instalate pe toate stațiile și serverele din rețea, evitând posibile probleme ce pot afecta serverele sau stațiile critice. Astfel, serverul de actualizare include 2 tipuri de actualizări de produs: a. Ciclu rapid, gandit pentru un mediu de test în cadrul rețelei b. Ciclu lent, gândit pentru restul rețelei (producție, servere critice etc) 8. Soluția permite stabilirea zonelor de test și critice din cadrul rețelei prin intermediul politicilor din consola de management. K. Certificate: 1. Accesul la consola de management sa se faca doar prin HTTPS. 2. Serverul web, din consola centrală de management trebuie să permită importarea de certificate digitale eliberate de o autoritate de certificare autorizată sau proprie organizației. 3. Soluția permite afișarea în consola de management de informații despre certificate: nume, autoritatea emitentă, data eliberării și data expirării certificatelor eliberate. L.API 1. Soluția va permite administratorului sa efectueze „call-uri" API 2. Soluția va include metode de management a conturilor de utilizator, a notificărilor, grupurilor de endpoint-uri, a politicilor respectiv a generarii de rapoarte prin intermediul cheilor API.		
	B. PROTECTIE STATII SI SERVERE FIZICE/VIRTUALE	I. Caracteristici generale minimale și eliminatorii: 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 fără modulul de control al accesului web, modul de control al dispozitivelor sau modulul firewall). 2. Pentru o mai bună protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigură protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare. 3. Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului Antimalware.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		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). 5. Pentru o mai bună protectie 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. 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. Fiecărui tip de amenințare menționat, i se vor putea stabili, independent, un nivel de protectie dorit: permisiv, normal, agresiv. 7. Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, șterge sau muta în carantină pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide dacă dorește întâi monitorizare sau dorește și blocarea amenințărilor. Aceste 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). 8. Pentru a oferi un nivel adițional de protecție a stațiilor și serverelor, soluția include un sandbox în cloud-ul public al producătorului acesteia. 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. 10. Modulul de Sandbox include două variante de analiză: doar monitorizare sau blocare. În modul monitorizare utilizatorul va putea accesa fișierul dorit, pe cand în modul blocare, utilizatorului i se va bloca rularea fișierului până când Sandbox-ul din cloud-ul producătorului va da verdictul. 11. Modulul de Sandbox include două tipuri de acțiuni remediere: implicită și de siguranță. Pentru acțiunea implicită se va putea stabili: doar raportare, dezinfecție, ștergere și carantinare. Pentru acțiunea de siguranță se va putea stabili: ștergere sau carantinare. 12. Modulul de Sandbox include și posibilitatea de trimitere manuală a fișierelor în Sandbox-ul din cloud-ul producătorului. Astfel, dacă administratorul suspectează un fișier ca fiind malițios, îl poate trimite manual în Sandbox pentru a fi „detonat" și a afla verdictul. Va putea trimite mai multe fișiere deodată, cu posibilitate de a specifica dacă vor fi „detonate" individual sau toate în același timp. 13. Modulul de Sandbox poate suporta „detonarea" următoarelor tipuri de fișiere: 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. 14. Fișierele menționate 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 Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ. 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. 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 funcțional modulul EDR cuprinde 2 componente distincte: senzorul ce colectează și procesează datele respectiv partea de analiză de securitate care are ca obiect interpretarea acestora. 17. Modulul EDR are capacitatea de a evalua activitatea tipică a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		(„baselining") și poate raporta orice deviație de la acest comportament sub forma unui incident. 18. Modulul EDR permite filtrarea incidentelor din interfața grafică în funcție de 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. 19. Modulul EDR permite vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat după cum urmează: tab-ul „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, investigații – virus total, sandbox, google – la nivel de fișier, adăugare în lista de blocare – la nivel de rețea sau instalare patch – la nivel de nod). 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. 21. Modulul EDR poate excepta fișiere non-malitioase de la acțiunea de investigare sau poate genera/adăuga un set de fișiere malițioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase. 22. Modulul EDR permite deschiderea unei conexiuni remote către un endpoint potențial infectat pentru a permite o investigare rapidă a gazdei, a colecta date despre atac, respectiv a remedia în timp real breșe de securitate eliminând astfel posibile incertitudini privitoare la comportamentul potențial malițios al unor fișiere/procese, reducând timpul de remediere (downtime), în cazul în care un atac a avut succes și stația ținta trebuie reconfigurată/reinstalată, permite executarea unor comenzi în linia de comandă care se execută cu privilegii de kernel ce permit eliminarea în timp real a unor amenințări sau colectarea de date privitoare la atacul în desfășurare. 23. Modulul EDR permite crearea regulilor de detecție customizabile bazate pe procese, fișiere, regiștri și conexiuni de rețea. 24. Modulul EDR permite creare regulilor de excludere customizabile bazate pe procese, fișiere, regiștri și conexiuni de rețea. 25. Modulul EDR permite căutarea proactivă pe stațiile de lucru protejate a indicatorilor de compromitere precum hash-uri, nume de fișiere, nume de procese, chei de regiștri, valori de regiștri. 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. 27. Modulul de tip host IPS va reprezenta o sursa de telemetrie / date despre atac pentru modulul de tip EDR, acesta din urmă având abilitatea de a integra informații despre acțiunile luate de către o potențială amenințare la nivel de rețea. II. Cerințe de sistem: Sisteme de operare pentru stații de lucru: Windows 11, Windows 10, Windows 8/8.1, Windows 7, Mac OS Monterey 12.x, macOS BIG SUR 11.x, macOS Catalina 10.15, Mac OS X Mojave (10.14), Mac OS High Sierra (10.13), Mac OS Sierra (10.12), Sisteme de operare embedded: Windows 10 IOT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7,Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7 Sisteme de operare pentru servere: Windows Server 2022, Windows Server 2019, Windows Server 2019 CORE, Windows Server 2016 , Windows Server 2016 (Core), Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, , Windows Server 2008 R2, Sisteme de operare Linux: Red Hat Enterprise Linux 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau mai recent, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Enterprise 15 SP2,SP3, OpenSUSE LEAP 15-2-15.3., Fedora 31 sau mai recent, AWS Bottlerocket 2020.03, Amazon Linux v2, Google COS Milestones 77,81,85, Azure Mariner 2, Alma Linux 8,9.x, Rocky Linux 8.x, Cloudlinux 7,8.x, Pardus 21, Linux Mint 20.3, Miracle 8.4.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		III. Administrare și instalare remote: Înainte de instalare, administratorul va putea particulariza pachetele de instalare cu modulele dorite: advanced threat control, anti-exploit, firewall, network protection respectiv content control, device control, power user, patch management, full disk encryption, EDR sensor, exchange protection respectiv „relay" (cu sau fără „patch caching server") Instalarea se va putea face în mai multe moduri: a. prin descărcarea directă a pachetului pe stația pe care se va face instalarea; b. prin instalarea la distanță, direct din consola de management c. trimiterea pe email (oricate adrese) a pachetului de instalare pentru Windows, Linux, Mac. Instalarea clienților la distanță în alte locații decât cele în care este instalată consola de management se va face prin intermediul unui alt client antivirus existent în locațiile respective pentru a minimiza traficul în WAN. În consolă vor fi disponibile informații despre fiecare stație: numele stației, IP, sistem de operare, module instalate, politică aplicată, informații despre actualizări etc. Din consolă se va putea trimite o singura politică pentru configurarea integrală a clientului de pe stații/servere. Consola va 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. Posibilitatea creării unui singur pachet de instalare, utilizabil atât pentru sistemele de operare pe 32 de biți cât și pentru cele pe 64 de biți. Posibilitatea creării unui singur pachet de instalare, utilizabil pentru stații (fizice și/sau virtuale), servere (fizice și/sau virtuale), Microsoft Exchange. Posibilitatea de a crea pachetele de instalare de tip web installer sau kit full. Administratorul va putea crea grupuri sau chiar subgrupuri, unde va putea muta stațiile/serverele din rețea pentru cele care nu sunt integrate domeniu. Permite selectarea clientului care va realiza descoperirea stațiilor din rețea, altele decat cele integrate în domeniu. Permite raportarea stațiilor care sunt protejate respectiv neprotejate de către soluție. Permite definirea de portlet-uri (reprezentări grafice) configurabile. Permite crearea și existența a 2 grupuri separate de conturi de utilizator, diferenta între acestea fiind data de existență sau nu a privilegiilor de administrator. IV. Caracteristici și funcționalități principale ale modulului antimalware și antispyware 1. Soluția permite administratorului sa stabilească acțiunea luată de produsul Antimalware la detectarea unei amenințări noi. Astfel administratorul va putea alege între următoarele acțiuni: a. Acțiune implicită pentru fișiere infectate: - interzice accesul - dezinfectează - ștergere - muta fișierele în carantină - nicio acțiune b. Acțiune alternativă pentru fișierele infectate: - interzice accesul - dezinfectează - ștergere - mută fișierele în carantină c. Acțiune implicită pentru fișierele suspecte: - interzice accesul - ștergere - mută fișierele în carantină - nicio acțiune d. Acțiune alternativă pentru fișierele suspecte:		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		- interzice accesul - ştergere - mută fişierele în carantină 2. Scanarea automată în timp real va putea fi setată să nu scaneze arhive sau fişiere mai mari de o anumită valoare, mărimea fişierelor putând fi definită de administratorul soluției, 3. Definirea pana la 16 nivele de profunzime pentru scanarea în arhive. 4. Scanarea euristică comportamentală prin simularea unui calculator virtual în interiorul căruia sunt rulate aplicații cu potențial periculos protejand sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă. 5. Scanarea oricărui suport de stocare a informației (CD-uri, harduri externe, unități partajate etc). De asemenea, se va putea anula scanarea în cazul în care sunt detectate unități care au informații stocate mai mult de o anumită valoare, mărimea fişierelor putând fi definită de administratorul soluției. 6. Scanarea automată a email-urilor la nivelul stației de lucru pentru POP3/SMTP. 7. Configurarea căilor ce urmează a fi scanate la cerere. 8. Clienții antimalware pentru workstation să permită definirea unor liste de excludere de la scanarea în timp real şi la cerere a anumitor directoare, discuri, fişiere, certificate, extensii sau procese, incluzând amprenta (hash) în cazul fişierelor sau certificatelor. 9. Cu ajutorul unei baze de date complete cu semnături de spyware şi a euristicii de detecție a acestui tip de programe, produsul va trebui să ofere protecție anti-spyware. 10. Posibilitatea de configura scanarile programate sa se execute cu prioritate redusă. 11. Produsul antimalware poate fi configurat să folosească scanarea în cloud, şi parțial scanarea locală. Pentru stațiile ce nu au suficiente resurse hardware, scanarea se poate face cu o maşină de scanare instalată în rețea. 12. Administratorul poate personaliza şi motoarele de scanare, având posibilitatea de a alege între mai multe tehnologii de scanare: · Scanare locală, când scanarea se efectuează pe stația de lucru locală. Modul de scanare locală este potrivit pentru maşinile puternice, având toate semnăturile şi motoarele stocate local. · Scanarea hibrid cu motoare light (Cloud public), cu o amprentă medie, folosind scanarea în cloud şi, parțial, semnături locale. Acest mod de scanare oferă avantajul unui consum mai bun de resurse, fără să implice scanarea locală. · Scanarea centralizată în Cloud-ul privat, cu o amprentă redusă, necesitând un server de securitate pentru scanare. În acest caz, nu se stochează local nicio semnătură, iar scanarea este transferată către serverul de securitate. · Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare locală (motoare full) · Scanare centralizată (Scanare în cloud privat cu server de securitate) cu fallback* pe Scanare hybrid (cloud public cu motoare light) 13. Pentru o protecție sporită, soluția antimalware trebuie să aibă 3 tipuri de detecție: bazată pe semnături, bazată pe comportamentul fişierelor şi bazată pe monitorizarea proceselor. 14. Pentru o protecție sporită, soluția antimalware trebuie să poată scana paginile HTTP (incluzand SSL). 15. Pentru o mai bună gestionare a antimalware instalat pe stații, produsul va include opțiunea de setare a unei parole pentru protecția la dezinstalare. 16. Pentru siguranța utilizatorului, clientul va include un modul de antiphishing (acesta va putea verifica linkurile indexate şi prezentate utilizatorului în urma unei căutări) 17. Soluția oferă protecție în timp real pe maşinile cu sistem de operare Linux în conformitate cu versiunea de kernel instalată. 18. Soluția va oferi o tehnologie de tip „preventiv / vaccin" ce va acționa împotriva potențialelor atacuri de tip ransomware. 19. Soluția va oferi un set de excluziuni predefinite pentru Roluri de tip „server" Microsoft (DNS, DHCP, AD, Exchange, Sharepoint)		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		20 Soluția va putea detecta atacuri de tip „file-less" incluzând pe cele ce folosesc utilitare aferente sistemelor de operare de tip interpretor de script (powershell). Soluția nu va bloca în mod uzual scripturi pentru a proteja împotriva acestor tipuri de atacuri. 21. Soluția va oferi un modul adițional de securitate bazat pe algoritmi tunabili de machine learning respectiv algoritmi euristici agresivi capabili să detecteze și blocheze atacuri de tip persistent sau targetat precum și alte categorii de malware sofisticat înainte de faza de execuție. Acest modul oferă următoarele funcționalități: a.Clasificarea tipului de atac b.Abilitatea de a raporta amenințările detectate fără a le bloca c.Abilitate de a ajusta agresivitatea detecției pe cel puțin 3 nivele (incluzând posibilitatea de a raporta atacuri ce ar fi fost blocate pe un nivel de agresivitate a detecției „mai ridicat" decât cel setat în mod curent în modul). d. Abilitatea de a acționa în mod diferit în funcție de tipul amenințării (fișier sau atac prin rețea) 22. Soluția oferă posibilitatea de restaurare a fișierelor modificate de un proces suspicios/necunoscut cu comportament de ransomware, odată ce soluția determină că procesul este malițios. 23. Soluția oferă protecție împotriva atacurilor ransomware inițiate la distanță, de pe alte stații de lucru (de exemplu: încercarea de atac ransomware pe un share de pe o stație de lucru care are acces la share). V. Anti-Exploit-Avansat 1. Posibilitatea de a opri atacurile avansate de tip „zero-day" efectuate prin intermediul unor exploit-uri evazive 2. Depistarea în timp real a celor mai recente exploit-uri ce pot vulnerabiliza un sistem de operare. 3. Protejarea aplicațiilor utilizate frecvent și a celor de tip „sistem" cum ar fi browserele, aplicațiile de tip office sau reader, procesele critice aferente sistemelor de operare. VI. Firewall 1. Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate. 2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 3. Posibilitatea de a defini rețele de încredere pentru mașina destinație. 4. Abilitatea de a detecta scanarea de porturi. 5. Posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide) 6. Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune VII. Carantina 1. Produsul antimalware să permită trimiterea automată a fișierelor din carantină către laboratoarele antimalware ale producătorului. 2. Trimiterea conținutului carantinei va putea fi expediat în mod automat, la un interval definit de administrator. 3. Produsul antimalware să permită ștergerea automată a fișierelor carantinate mai vechi de o anumită perioadă, pentru a nu încărca inutil spațiul de stocare. 4. Posibilitatea de a restaura un fișier din carantină în locația lui originală. 5. Modulul de carantină va permite rescanarea obiectelor după fiecare actualizare de semnături. 6. Modulul de carantină va permite salvarea unei copii a fișierului infectat respectiv transmiterea acestuia către carantină înainte de a efectua orice altă acțiune asupra acestuia. VIII. Protecția datelor 1. Produsul permite blocarea datelor confidențiale (pin-ul cardului, cont bancar etc) transmise prin HTTP sau SMTP prin crearea unor reguli specifice.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		IX. Controlul conținutului Consola va avea integrat un modul dedicat controlului accesului la Internet cu următoarele particularități: a. Permite blocarea accesului la Internet pentru anumite masini client sau grupuri de mașini. b. Permite blocarea accesului la Internet pe intervale orare. c. Permite blocarea paginilor de internet care conțin anumite cuvinte cheie. d. Permite controlul accesului numai la anumite pagini de internet specificate de administrator; e. Permite blocarea accesului la anumite aplicații definite de administrator; f. Permite restrictionarea accesului pe anumite pagini de internet după anumite categorii prestabilite (ex: online dating, violenta, pornografie etc). X. Controlul dispozitivelor 1. Modulul previne scurgerea accidentală sau intenționată de date respectiv potențiale infecții cu malware prin atașarea de dispozitive externe. 2. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 3. Modulul va permite controlul următoarelor tipuri de dispozitive: a. Bluetooth Devices b. CDROM Devices c. Floppy Disk Drives d. Security Policies 153 e. IEEE 1284.4 f. IEEE 1394 g. Imaging Devices h. Modems i. Tape Drives j. Windows Portable k. COM/LPT Ports l. SCSI Raid m. Printers n. Network Adapters o. Wireless Network Adapters p. Internal and External Storage 4. Modulul permite capturarea unor informații specifice legate de dispozitivele externe cum ar fi: nume, class ID, momentul în timp când a fost conectat 5. Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașina client cum ar fi: permis/blocat/custom respectiv poate limita accesul dispozitivelor externe la „read only" sau limita doar accesul la porturile USB ale endpoint-ului permițând orice alt tip de dispozitiv ce nu folosește acest tip de port/interfață. 6. Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli pe baza Product/Device/Hardware ID. 7. Modulul poate „descoperi" noi dispozitive și raporta prezența acestora în consola de management. XI. Power User 1. Modulul poate fi instalat/dezinstalat în funcție de preferința administratorului. 2. Modulul permite posibilitatea de a acorda utilizatorilor drepturi de Power User. Utilizatorii vor putea accesa și modifica setarile clientului antimalware dintr-o consola disponibilă local pe mașina client. 3. Modificările efectuate din modulul Power User vor fi active local, pe mașina pe care s-au făcut respectivele modificări. 4. Administratorul va putea suprascrie din consolă setarile aplicate de utilizatorii Power User. XII. Actualizare		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		Posibilitatea efectuării actualizării la nivel de stație în mod silențios (fără avertizare). Sistem de actualizare cascadat folosind unul sau mai multe servere de actualizare (cascadate). Actualizarea pentru locațiile remote prin intermediul unui client antimalware care are și rol de server de actualizare. Abilitatea de a împiedica punctele finale să iasă pe internet pentru a descărca actualizări. XIII. Protecție pentru Dispozitive de Stocare Externe 1. Soluția trebuie să poată proteja dispozitive de stocare externe ce suportă ICAP (Internet Content Adaptation protocol, așa cum a fost definit acesta în RFC 3507) 2. Soluția trebuie să ofere protecție antimalware pentru fișiere stocate pe orice dispozitiv de stocare extern compatibil ICAP 3. Soluția trebuie să ofere mai multe nivele de apărare împotriva amenințărilor bazate pe algoritmi de tip machine learning, euristici, semnături precum și informații obținute din cloud-ul de tip „threat intel" al producătorului. 4. Soluția trebuie să poată proteja dispozitivele de stocare externe împotriva amenințărilor necunoscute (pentru care nu exista o semnătură) 5. Soluția va oferi scanare la acces pentru dispozitivele de stocare externe 6. Soluția va oferi scanare la acces pentru arhive stocate pe dispozitive de stocare externe cu opțiuni configurabile cum ar fi mărimea maximă a arhivei sau nivelul de adâncime a acesteia (cel puțin 64 de nivele de adâncime vor fi permise) 7. Soluția va pune la dispoziția administratorului cel puțin 2 metode prin care să se prevină supraincarcarea serverului de scanare respectiv cel puțin 2 acțiuni ce pot fi luate în momentul în care a fost identificat un fișier infectat pe un dispozitiv de stocare extern. XIV. Modul pentru managementul patch-urilor pe stațiile de lucru (ADD-ON) 1. Capacitatea de a funcționa în modul automat a. Programarea scanărilor pentru patch-ul lipsă b. Programarea instalării automată separată pe baza categoriei de patch-uri (securitate / non-securitate) c. Posibilitatea de a amâna repornirea stațiilor de lucru, dacă instalarea patch-ului o solicită. 2. Soluția trebuie să permită modul manual - descoperirea și instalarea patch-urilor la cerere 3. Soluția trebuie să ofere posibilitatea de a vedea toate patch-urile care lipsesc din mediu. Aceste informații ar trebui să fie agregate într-un inventar de patch-uri. a. Soluția va oferi vizibilitate a punctelor finale instalate sau lipsește un patch specific. b. Soluția va oferi informații și motive în cazul în care un patch nu se instalează c. Soluția va oferi utilizatorului posibilitatea de a instala rapid patch-urile lipsă d. Utilizatorul ar trebui să poată lista neagră unul sau mai multe patch-uri. 4. Soluția va oferi raportarea patch-urilor lipsă din perspectiva punctului final (patch-uri instalate / lipsă pe fiecare punct final) 5. Soluția va trimite notificări periodic, dacă pe stațiilor de lucru lipsesc patch-uri. 6. Soluția va oferi posibilitatea de stocare a patch-urilor pe o masina special desemnată (caching server), în acest fel patch-urile vor fi descărcate de pe internet numai de către unele puncte finale atribuite. XV. Modul pentru criptarea discurilor (Full Disk Encryption) – (ADD-ON) 1. Soluția trebuie să accepte criptarea completă a discului. 2. Folosește criptare nativă compatibilă cu Windows și MAC OS 3. Soluția impune autentificarea pre-boot cu parolă		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		4. Soluția gestionează cheile de recuperare în cazul în care utilizatorii își uită parolele. 5. Soluția oferă rapoarte pentru a demonstra conformitatea cu setările de criptare XVI. Controlul aplicațiilor: 1. Pentru o mai bună inventariere și administrare, soluția va include o secțiune în consola de administrare unde se vor regăsi toate aplicațiile descoperite în rețea, grupate după: nume, versiune, descoperit la, găsit pe. 2. Pentru o mai bună inventariere și administrare, soluția va include o secțiune în consola de administrare unde se vor regăsi toate procesele negrupate descoperite în rețea, grupate după: nume, versiune, nume produs, versiune produs, editor/autor, descoperit la, găsit pe. 3. Pentru prevenirea infectării stațiilor și serverelor dar și pentru a permite aplicațiilor descoperite în rețea să se poată actualiza, soluția permite definirea unor programe de actualizare (Updater) care vor fi lăsate sa actualizeze diferite aplicații instalate pe stații sau servere. 4. Acest modul poate funcționa în modul Whitelisting (prin care se blochează accesul la toate aplicațiile cu excepția celor menționate în lista alba) sau Blacklisting (prin care se blochează doar accesul la aplicațiile menționate în lista neagră). 5. Soluția include opțiunea de a permite sau a bloca rularea anumitor aplicații sau procese definite de administrator (inclusiv subprocese) după: a. Cale fișier: local, CD-ROM, portabil sau rețea b. Hash c. Certificat		
	C. PROTECȚIA PENTRU POSTURILE DE MUNCĂ ȘI SERVICII VIRTUALIZATE	A. Protecție antimalware dedicată mediilor virtualizate - cerințe minime: 1.Produsul se integrează cu aplicația de virtualizare ofertată de Ofertant și oferă posibilitatea scanării antimalware fără a instala un agent de scanare pe mașina virtuală. 1. Componenta de gestionare centrală a soluției se integrează cu mai multe medii virtuale. 2. Pentru toate sistemele care rulează sisteme de operare, produsul include: a. Scanarea proceselor; b. Scanarea memoriei; c. Scanare în timp real a fișierelor; d. Scanați fișiere la cerere; 3. Scanare în timp real și la cerere pentru mașini virtuale cu sisteme de operare. 4. Introspecție sistem operare prin aplicația de virtualizare ofertată de Ofertant. 5. Produsul este compatibil, de asemenea, VMWARE, Microsoft Hyper-V, Red Hat Virtualization, Oracle VM și KVM. 7. Produsul trebuie să includă o singură mașină de scanare virtuală care: a. Conține semnăturile antimalware; b. Oferă protecție completă, actualizată, la deschiderea unei mașini virtuale; c. Oferă scanare optimizată. B. Caracteristici generale: 1. Metode de detectare a virușilor, spyware-urilor, rootkiturilor și a altor programe malware. 2. Produsul trebuie să permită actualizarea automată a dispozitivului virtual de securitate, pentru semnăturile antimalware și pentru sistemul de operare al dispozitivului virtual de securitate. 3. Produsul trebuie să raporteze starea curentă a gazdei de securitate - aparate virtuale protejate / neprotejate și de securitate virtuale. C. Cerințe minime de sistem: 1. Platforme de virtualizare: VMware vSphere și vCenter Server versiuni: version 6.5 version 6.7, incluzand update 1, update 2a și update 3 version 7.0, incluzand update 1, update 2, update 2b, update 2c și update 2d VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x VMware Workstation 11.x, 10.x, 9.x, 8.0.6		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		VMware Player 7.x, 6.x, 5.x Citrix Xen Hypervisor: 7.1 (with the XS71ECU2060 hotfix), 8.2. Citrix Virtual Apps and Desktops 7 1808, 7 1811, 7 1903, 7 1906 Citrix XenApp and XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR Citrix VDI-in-a-Box 5.x Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (including Hyper-V Hypervisor) Red Hat Enterprise Virtualization 3.0 (including KVM Hypervisor) Oracle VM 3.0 Oracle VM VirtualBox 5.2, 5.1 Nutanix Prism with AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition) Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 and 20190916.294 (Community Edition) 2. Sisteme de operare pentru mașini virtuale (32/64 biți): Sisteme de operare pentru stații de lucru: Windows 11, Windows 10, Windows 8/8.1, Windows 7, Mac OS Monterey 12.x, macOS BIG SUR 11.x, macOS Catalina 10.15, Mac OS X Mojave (10.14), Mac OS High Sierra (10.13), Mac OS Sierra (10.12), Sisteme de operare embedded: Windows 10 IOT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7,Windows Embedded POS Ready 7 Windows Embedded POSReady 7, Windows Embedded Enterprise 7 Sisteme de operare pentru servere: Windows Server 2022, Windows Server 2019, Windows Server 2019 CORE, Windows Server 2016 , Windows Server 2016 (Core), Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, , Windows Server 2008 R2, Sisteme de operare Linux: Red Hat Enterprise Linux 7.x, 8.x,9.x, CentOS 7.x, 8.x, Ubuntu 16.04 sau mai recent, SUSE Linux Enterprise Server 12SP4,5, SUSE LINUX Enterprise 15 SP2,SP3, OpenSUSE LEAP 15-2-15.3., Fedora 31 sau mai recent, AWS Bottlerocket 2020.03, Amazon Linux v2, Google COS Milestones 77,81,85, Azure Mariner 2, Alma Linux 8,9.x, Rocky Linux 8.x, Cloudlinux 7,8.x, Pardus 21, Linux Mint 20.3, Miracle 8.4. D. Principalele caracteristici și funcționalități ale modulului antimalware: 1. Scanarea automată a fișierelor care sunt copiate pe suport extern și de pe LAN sau WAN. 2. Scanarea automată în timp real a fișierelor poate fi setată pentru a scana numai anumite tipuri de fișiere, cu extensii specifice, definite de administrator. 3. Scanarea automată în timp real a fișierelor poate fi setată pentru a nu scana arhive mai mari de o anumită valoare, mărimea fișierelor putând fi definită de administratorul soluției. 4. Scanarea la cerere va include următoarele opțiuni: i. Scanați orice suport de stocare conectat la mașina virtuală; ii. Scanarea emailurilor; 5. Configurarea căilor de scanat, la nivelul fișierului; 6. Trebuie să permită administratorului să definească anumite foldere, discuri, fișiere și extensii care să fie excluse de la scanarea în timp real și la cerere. 7. Pentru a nu supraîncărca resursele sistemului, produsul antimalware trebuie să conțină un singur motor de scanare. 8. Pentru a permite optimizarea cantității de trafic trimis către rețea printr-un mecanism de cache pe mașina de scanare și pe mașina virtuală. 9. Conexiuni de reluare / echilibrare a sarcinii agentului la mașina de scanare. 10. Politicile pot fi aplicate unui pool de resurse din aplicația de virtualizare ofertată de Ofertant.. E.Carantină: 1. Produsul antimalware trebuie să permită ștergerea automată a fișierelor în carantină mai vechi de o anumită perioadă, fără a ocupa spațiu de stocare inutil. 2. Posibilitatea de a muta un fișier din carantină în locația inițială. 3. Carantină centralizată. Capacitatea de a aduna în siguranță toate fișierele din carantină de la punctele finale protejate la o locație unică în rețea pentru o investigație mai profundă.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		4. Posibilitatea de a descărca fișierul direct pe stația de lucru a administratorului (numai pentru integrarea cu aplicația de virtualizare ofertată de Ofertant). 5. Posibilitatea de a resana fișierele în carantină după fiecare actualizare a semnăturii. 6. Posibilitatea trimiterii automate de fișiere din carantină către laboratoarele producătorilor la un interval de timp stabilit de administrator. F.Management și instalare la distanță: 1. Aparatul virtual de securitate poate fi personalizat înainte de instalare. Acesta este scalat automat în funcție de mai multe caracteristici: numărul de mașini virtuale de pe gazdă, rețele, resurse alocate de adrese IP (CPU, memorie) etc. 2. Consola de administrare va raporta numărul de mașini virtuale care au instalat sau nu instalarea soluției de protecție antivirus și starea mașinii: Activat sau Dezactivat. 3. Posibilitatea consolei de administrare de a raporta dacă modulul antimalware este sau nu activat pe mașina virtuală.		
	D. PROTECȚIE ȘI SECURITATE PENTRU TELEFOANELE MOBILE DE TIP SMARTPHONE	1. Cerințe minime de sistem: • Telefoane cu sistem de operare iOS 8.1 sau mai nou: Apple iPhone și tablete iPad • Telefoane sau tablete cu sistem de operare Android 4.0.3 sau mai nou 2. Caracteristici: a. Permite asocierea unui dispozitiv cu un utilizator din Active Directory. b. Instalarea se face prin trimiterea unui email către utilizator cu detaliile de instalare. c. Activarea dispozitivului mobil în consola de management să se facă prin scanarea unui cod QR. d. Pachetele de instalare se vor putea descărca de pe Apple App Store și Google Play. e. Se vor putea întreprinde următoarele acțiuni: i. Blocarea dispozitivului; ii. Deblocarea dispozitivului; iii. Ștergerea datelor și revenirea la setările din fabrică; iv. Localizarea dispozitivului; v. Scanarea dispozitivului(doar pentru cele cu sistem de operare Android); vi. Criptarea memoriei dispozitivului(doar pentru cele cu sistem de operareAndroid). f. Consola va permite raportarea dispozitivelor: active, inactive, deconectate, cu sistemul de operare modificat astfel încât utilizatorul să aibă acces total asupra lui (rooted or jailbroken devices). 3. Setări de securitate: A. În cazul în care un dispozitiv nu este conform cu setarile dorite, se vor putea întreprinde automat acțiunile: a. Ignorare; b. Blocarea accesului; c. Blocarea dispozitivului; d. Ștergerea datelor și revenirea la setările din fabrică; e. Ștergerea dispozitivului din consola. B. Se va putea impune blocarea dispozitivelor cu ajutorul unei parole. Aceasta parolă va putea fi configurată să conțină: a. Parola simplă sau complexă (în funcție de cerințele sistemului de operare); b. Numere și litere; c. O lungime minimă definită de administrator; d. Un număr minim de caractere speciale, definit de administrator; e. Perioada de expirare a parolei. Perioada va putea fi definită de administrator; f. Configurarea restricției refolosirii parolei; g. Numărul de introduceri incorecte a parolei, de către utilizator;		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		h. Perioada de autoblocare a dispozitivului după un număr de minute definite de administrator. C. Se vor putea genera mai multe profiluri care vor stabili reguli de securitate pentru conectivitatea la Wi-Fi sau VPN (numai pentru sistemul de operare iOS) dar și unele legate de accesul la anumite pagini de internet. D. Profilurile de Wi-Fi vor conține următoarele opțiuni: a. Generale – se definește SSID precum și tipul securității rețelei; b. Setări TCP/IP – atat pentru protocolul IPv4 dar și pentru IPv6; c. Setari de proxy – dezactivat, automat sau configurat manual. E.Profilurile acces pagini de internet pentru sistemul de operare Android includ opțiuni precum: a. Permiterea, blocarea sau programarea pentru anumite zile și intervale orare a accesului la anumite pagini de internet; b. Crearea unor excepții pentru blocarea sau permiterea accesului către anumite pagini de internet. F.Profilurile acces pagini de internet pentru sistemul de operare iOS includ opțiuni de activare sau dezactivare a: a. Utilizarii browser-ului Safari; b. Opțiunii de completare automată a informațiilor; c. Alertarii utilizatorului în cazul accesării unor pagini frauduloase; d. Javascript; e. Pop-up-urilor		
	E. PROTECȚIE ȘI SECURITATE PENTRU SERVERELE EMAIL MICROSOFT EXCHANGE	1. Cerințe minime de sistem: • Exchange server 2019, 2016, 2013 cu rol de Edge Transport sau Mailbox • Exchange server 2010 cu rol de Edge Transport, Hub Transport sau Mailbox 2. Produsul va oferi 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. Produsul va asigura scanarea atasamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanta serverului de mail. 4. Actualizarea antimalware trebuie să poată fi făcută automat la un interval de maxim 1 ora, precum și la cerere. 5.4. În afară de detecția pe bază de semnături, modulul de protecție antimalware va trebui să includă și scanare euristica comportamentală, prin simularea unui calculator virtual în interiorul căruia sunt rulate și analizate aplicații cu potențial periculos, pentru a proteja sistemul de viruși necunoscuți prin detectarea codurilor periculoase a căror semnătura nu a fost lansată încă. 6. Produsul va oferi opțiuni multiple de acțiune la identificarea unui atașament virusat (dezinfectare, ștergere, mutare în carantină). 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. 8. Produsul va oferi protecție antispam, cu o bază de semnături actualizabilă prin internet. 9. Modulul antispam va trebui 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. 10. Produsul va trebui sa 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. 11. Produsul va trebui să ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute. 12. Produsul va oferi posibilitatea de a defini politici de filtrare antimalware, antispam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori.		

Nr Crt	Caracteristică	Cerințe minimale obligatorii	UM	Cantitate
		13. Actualizarea produsului va fi configurabilă și se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu. 14. Produsul va trebui să ofere statistici atat referitoare la scanarea antivirus cât și la scanarea antispam. 15. Produsul se va integra în cadrul consolei de management unitar al soluției antivirus. Pentru ușurința accesului la setarile produsului din diferite medii de operare, produsul va avea consola de administrare web.		
16	**Alte componente informatice** Pentru a se reduce impactul bugetar al proiectului și a se realiza mediile informatice tip Centre de date atat pentru sistemul de producție cat și pentru cel de back-up și recuperare în caz de incidente, sunt necesare a fi achizitionate următoarele componente ce vor fi instalate de către Furnizor pe serverele existente ale Autoritatii Contractante, detaliile acestor echipamente se regasesc în Anexa 1.1, puse la dispoziție pentru acest proiect, astfel:			
	7Y37A01090	ThinkSystem 430-8e SAS/SATA HBA	Buc	5
	7ZT7A00537	ThinkSystem Intel X710-DA2 PCIe 10Gb 2-Port SFP+ Ethernet Adapter	Buc	4
	46C3447	SFP+ SR Transceiver, transcieverele fiind de la același producător sau recomandate de producătorul echipamentului	buc	8
	00MN505	Lenovo 3m LC-LC OM3 MMF Cable	buc	8
		Patchcord fibră optică multi mode OM3, conectori duplex LC-SC min 2m	buc	16
		Patchcord fibră optică multi mode OM3, conectori duplex LC-SC min 5m	buc	5
		Rack 19 inch 42U cu montare pe podea, ușă din sticlă, panouri laterale detașabile și securizate, asamblat cu accesoriile necesare: -Modul ventilație plafon 2 fan + cablu, interconectabil, -2xGhidaj/Organizator orizontal 5 inele, 1U 19 inch, metalic, -10x Raft fix capacitate ridicată pentru rack -4x Bară alimentare / PDU, 19 inch, prize Schuko + switch, 16A, 3500W -1xTermostat digital pentru rack de podea cu prindere in plafon -4x Patch panel 24 porturi, suport de cabluri integrat	buc	1
		Patchcord fibră optică multi mode OM3, conectori duplex LC-LC, 0.5m	buc	4
		Patchcord fibră optică single mode OS2, conectori duplex LC-LC, 5m	buc	8
17	**Circuit nou de FO**		**set**	**1**
		Circuit nou de FO cu o lungime de aproximativ 300 m cu minim 6 perechi de fibre (adică 12 fibre optice), patch paneluri și conectori pentru toate fibrele, și accesoriile de montaj, întinzătoare cablu și traversare aeriană circuit de FO. Patch Panelurile trebuie să acomodeze toate fibrele sudate, să le organizeze în perechi (o fibra Tx, una Rx), și să permită conectarea cu patch-urile având conectori LC pentru toate fibrele.		

Întocmit,

Șef birou achiziții
Lt.cdor. Schipor Constantin

Șef comunicații și informatică
Col. Bucur Eugen

Verificat concordanța prevederilor Caietului de sarcini cu necesitățile obiective ale Academiei Navale „Mircea cel Bătrân”,
Cdor
Paul BURLACU