

TEHNIČKA SPECIFIKACIJA

	KARAKTERISTIKE		ZAHTJEV	ODGOVOR da/ne	
1.	Opća specifikacija				
1.1.1	Solution (Ime)				
1.1.2	Solution	Ponudeno rješenje mora biti jedinstven proizvod od jednog proizvođača	da		
1.1.3	Solution (Specify version & release date)	Ponudena verzija mora biti najnovija stabilna verzija dostupna na tržištu	da		
1.1.4	Solution	Ponudeno rješenje mora biti realizirano u cloud okruženju proizvođača	da		
1.2	Licensing	Ponudeno rješenje treba omogućiti najmanje 320 licenci za period od jedne (_1_) godine. Sve licence koje se nude moraju svi biti user based tj. license enforcement mora biti u centralnoj konzoli kako bi se u slučaju migriranja korisnika u okviru organizacije licenca ponovo mogla iskoristiti	da		
1.3.1	Support (specify vendor's local contact information)	Proizvođač Rješenje treba da ima lokalnog predstavnika preko koga će pružiti podršku.	da		
1.3.2	Support (specify number of engineers employed locally by the vendor)	Ponuditelj Rješenje (ili proizvođač) moraju imati zaposleno najmanje jednog (2) inženjera ponuđenog Rješenje kako bi pružili terensku podršku / daljinske sesije & pružaju e-mail / tehničku podršku ako bude potrebna s valjanim I važećim certifikatima proizvođača za davanje podrške.	da		
1.3.3	Support – product updates / upgrades	Proizvođač mora ponuditi besplatne Updates & Upgrades za vrijeme trajanja licenci (1 godina)	da		
1.3.4	product update / upgrade availability	Proizvođač mora ponuditi mogućnost preuzimanja najnovije verzije Rješenje , kao i sve ispravke, poboljšanja i dokumentaciju preko internet stranica proizvođača softwarea za vrijeme trajanja licenci (1 godina).	da		
1.3.5	Vendor Authorization	Da Ponuditelj ima važeću autorizaciju izdatu od strane Proizvođača software-a ili ovlaštenu ured/predstavništvo za Republiku Hrvatsku koji je predmet ove nabave	da		

	KARAKTERISTIKE		ZAHTJEV	ODGOVOR da/ne	
2.	Tehnička specifikacija za administrativnu konzolu				
2.1.1	Remote Management	Menadžment konzola za software mora biti web-based	da		
2.1.2	Remote Management	Pristup menadžment konzoli treba se obavljati preko SSL protokola	da		
2.1.3	Remote Management	Menadžment konzola mora biti dostupna samo ako se korisnik ulogira sa prethodno definiranim korisničkim imenom i lozinkom	da		
2.1.4	Remote Management	Menadžment konzola mora imati mogućnost kreiranja novih korisnika za pristup konzoli	da		
2.1.5	Remote Management	Menadžment konzola mora imati mogućnost definiranja različitih prava za korisnike koji su kreirani (npr. Monitoring, Basic Administration, Total Control itd)	da		
2.2	Update Configuration	Software za upravljanje mora podržavati napredno podešavanje za update, da update / upgrade se može provoditi u određenim intervalima ili u određeno vrijeme .	da		
2.3.1	Agent based deployment	Rješenje za upravljanje mora podržavati instalaciju, kompletnu administraciju i praćenje klijentskog softwarea preko agenta ili modula za upravljanje koji je nezavisan od softwarea za zaštitu klijenta.	da		
2.4	Remote Agent installation	Agent ili modul za upravljanje mora podržavati daljinsku instalaciju	da		
2.5	Manual Agent installation	Agent ili modul za upravljanje mora podržavati ručnu instalaciju	da		
2.6	Centralized Administration	Platforma mora biti u stanju da centralno upravlja svim klijentima na kojima su agenti (monitoring statusa klijenta, obavlja skeniranja i sl.) u intranet i internet okruženju	da		
2.7	Multiple Configurations support	Platforma mora omogućiti više konfiguracija i podršku grupama na koje oni će konfiguracije biti primenjene	da		
2.8	Profile Support	Platforma mora podržavati profile tako da omogući različite nivoe pristupa za administrativno osoblje	da		
2.9	Centralized Malware Activity Monitoring	Rješenje mora ponuditi mogućnost da se centralno prati aktivnost malware-a u realnom vremenu i generira statistika za posebne grupe na određenim periodima	da		
2.10	Centralized Event Logging	Platforma mora podržavati centralizirano vođenje evidencije događaja za malware događaje i sistemske događaja	da		
2.11	Centralized Quarantine	Platforma mora imati mogućnost centralnog upravljanja karatenom svih klijenata	da		
2.12	Centralized Reporting	Platforma mora podržavati centralizir kreiranje izvještaja	da		
2.13	Customizable Reports	Platforma mora podržavati stvaranje specijalizovanih (customised) izvještaja	da		
2.14	Report Export Capabilities	Platforma mora podržavati eksport izvještaja u standardnim formatima (npr . CSV , PDF , KSML)	da		

2.15	SMTP Notification Support	Zaštita krajnjih točaka mora podržavati obavijesti o događajima / logiranje preko SMTP	da		
2.16	Removal of competitive solutions (specify)	Endpoint agent mora imati mogućnost da uklanja software za zaštitu drugih proizvoda.	da		

	KARAKTERISTIKE		ZAHTJEV	ODGOVOR da/ne	
3.	Tehnička specifikacija klijentskog softwera za radne stanice				
3.1	Supported Operating Systems for Client Protection software	Windows 2000 Professional, Windows XP SP0 & SP1 (32 / 64-bits) XP SP2 ili kasniji (Vista, Windows 7 & Windows 8.1(32 / 64 bits & Windows 10 (32/64 bits),	da		
3.2	Installation / Uninstallation	Software za zaštitu klijenta ponuditi mogućnost i centralizirane i ručne instalacije	da		
3.3	Updates	Software za zaštitu klijenta mora biti u stanju da primi ažurirani signature file preko najbližeg računala u lokalnoj mreži ili direktno preko interneta ako paket za ažuriranje nije pronađen na LAN .	da		
3.4.1	Antimalware Protection	Software za zaštitu klijenta mora koristiti ili sisteme konvencionalne definicije zasnovane na skeniranje (na osnovu poznatih definicija i potpisa virusa, itd) ili dinamične cloud -based tehnike skeniranja	da		
3.4.2	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu i on-demand detekciju i dezinfekciju za sve file-ove i podatke I pokrenute aplikacije na lokalnim / mrežnim diskovima , u memoriji i boot sektorima	da		
3.4.3	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu tako i on-demand detekciju prijetnji u zapakiranim arhivima (npr zip, rar , cab itd)	da		
3.4.4	Antimalware Protection	Rješenje se mora integrirati sa mail klijentima i omogućiti u realnom vremenu i on-demand detekciju i dezinfekciju prijetnji otkrivenih u dolaznom / odlaznom prometu.	da		
3.5.5	Antimalware Protection	Rješenje mora omogućiti odvojene konfiguracije za file-ove i mail module za zaštitu	da		
3.4.6	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu tako i on-demand detekciju i dezinfekciju svih vrsta pretnji npr . Viruses, Worms, Trojans, Spyware, Malware, Adware, Hacking Tools itd	da		
3.4.7	Antimalware Protection	Rješenje mora ponuditi mogućnost da se specifični file-ovi / direktoriji ne skeniraju	da		
3.5.1	Firewall Protection	Rješenje mora ponuditi Firewall modul	da		
3.5.1.1	Firewall Protection	Rješenje mora ponuditi mogućnost da se Firewall zaštitom upravlja centralno iz konzole za upravljanje	da		
3.5.1.2	Firewall Protection	Rješenje mora da ponudi opciju da se Firewall zaštitom, upravlja i od strane klijenta, pored centralnog upravljanja iz konzole za upravljanje	da		

3.5.2	Firewall Protection	Rješenje mora ponuditi mogućnost da kontrolira pristup aplikacija Internetu	da		
3.5.3	Firewall Protection	Rješenje mora ponuditi mogućnost detekcije pokušaja upada (Intrusion detection).	da		
3.6.1	Device Control	Rješenje mora ponuditi mogućnost kontrole uređaja. Podržani uređaji moraju uključiti najmanje slijedeće tipove : <ul style="list-style-type: none"> • USB Keys • CD/DVD • Bluetooth uređaji • Image uređaji • USB Modemi 	da		
3.6.2	Device Control	Device Control modul mora omogućiti konfiguraciju različitih dozvola i mora ponuditi bar slijedeće mogućnosti: <ul style="list-style-type: none"> • Full Access • Read-only Access • Deny Access Completely 	da		
3.7	Web Filtering Protection	Rješenje mora ponuditi mogućnost da se kontrolira pristup site-ovima putem HTTP & HTTPS. Kontrola pristupa treba biti podešena odabirom unaprijed definirane kategorije (npr . Sport , pornografija , igre itd) site-ova koji se ažuriraju redovno.	da		
3.7.1	Web Filtering Protection	Rješenje mora ponuditi sposobnost kreiranja "bijelih lista", tako da se isključe određeni site-ovi iz blokade bez obzira da li pripadaju jednoj ili više kategorija koje su odabrane da budu blokirani	da		
3.7.2	Web Filtering Protection	Rješenje mora ponuditi sposobnost kreiranja "crnih lista", tako da se uvijek blokiraju određeni site-ovi definirani od strane administratora bez obzira da li pripadaju kategoriji koja je dozvoljena	da		
3.7.3	Web Filtering Protection	Rješenje mora ponuditi mogućnost da se definira da li će nekategorizirani (Unkown) site-ovi biti dozvoljeni ili blokirani	da		
3.7.4	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu tako i on-demand detekciju i dezinfekciju svih vrsta pretnji npr . Viruses, Worms, Trojans, Spyware, Adware, Hacking Tools, Cryptolocker, itd	da		
3.7.5	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu tako i on-demand detekciju pretnji u zapakiranim arhivima (npr zip, rar , cab itd)	da		

	KARAKTERISTIKE		ZAHTJEV	ODGOVOR da/ne	
4.	Tehnicka specifikacija klijentskog softwera za Server Platforms				
4.1	Supported Operating Systems for Client Protection software	Windows 2000 Server, Windows Home Server, Windows 2003 (32 / 64 bits & R2) SP1 and greater, Windows 2008 32 / 64 bits, Windows 2008 R2 (64 bits)), Windows Small Business Server 2011, Windows Server 2012 (64 bit & R2).	da		
4.2	Installation / Uninstallation	Software za zaštita klijenta mora ponuditi mogućnost i centralizirane i ručne instalacije	da		
4.3	Updates	Software za zaštitu klijenta mora biti u stanju primiti ažurirani signature file preko najbližeg računala u lokalnoj mreži ili direktno preko interneta ako paket za ažuriranje nije pronađen na LAN .	da		
4.4.1	Antimalware Protection	Software za zaštitu klijenta mora koristiti ili sisteme konvencionalne definicije zasnovane na skeniranje (na osnovu poznatih definicija i potpisa virusa, itd) ili dinamične cloud -based tehnike skeniranja	da		
4.4.2	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu i on-demand detekciju i dezinfekciju za sve file-ove i podatke na lokalnim / mrežnim diskovima , u memoriji i boot sektorima	da		
4.4.3	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu tako i on-demand detekciju prijetnji u zapakiranim arhivima (npr zip, rar , cab itd)	da		
4.4.4	Antimalware Protection	Rješenje mora integrirati sa mail klijentima i omogućiti u realnom vremenu i on-demand detekciju i dezinfekciju pretnji otkrivenih u dolaznom / odlaznom prometu.	da		
4.4.5	Antimalware Protection	Rješenje mora omogućiti odvojene konfiguracije za file i mail module za zaštitu	da		
4.4.6	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu tako i on-demand detekciju i dezinfekciju svih vrsta pretnji npr . Viruses, Worms, Trojans, Spyware, Malware, Adware, Hacking Tools itd	da		
4.4.7	Antimalware Protection	Rješenje mora ponuditi mogućnost da se specifični file-ovi / ekstenzije / direktoriji ne skeniraju	da		
4.5.1	Firewall Protection	Rješenje mora ponuditi Firewall modul	da		
4.5.1.1	Firewall Protection	Rješenje mora ponuditi mogućnost da se Firewall zaštitom upravlja centralno iz konzole za upravljanje	da		
4.5.1.2	Firewall Protection	Rješenje mora ponuditi opciju da se Firewall zaštitom, upravlja i od strane klijenta, pored centralnog upravljanja iz konzole za upravljanje	da		
4.5.2	Firewall Protection	Rješenje mora ponuditi mogućnost da kontroliše pristup aplikacija Internetu	da		
4.5.3	Firewall Protection	Rješenje mora ponuditi mogućnost detekcije pokušaja upada (Intrusion detection).	da		

4.5.4	Aplication control	Rješenje mora ponuditi automatsku provjeru i klasifikaciju SVIH pokrenutih aplikacija i servisa u realnom vremenu	da		
4.5.5	Aplication control	Rješenje mora ponuditi automatsku blokadu i klasifikaciju SVIH pokrenutih aplikacija i servisa prepoznatih kao mailware u realnom vremenu	da		

	KARAKTERISTIKE		ZAHTJEV	ODGOVOR da/ne	
5.	Technical Specifications of Antimalware Client Software For Exchange Server Platforms				
5.1	Supported Exchange Servers	Ponuđeno rješenje mora biti kompatibilno sa svim slijedećim Exchange Serverima: 2003 , 2007 , 2010 i 2013. Gdje god je potrebno, potrebna je 32 - bitna i 64 -bitna podrška	da		
5.2	Supported Exchange Environments	Ponuđeno rješenje mora biti u potpunosti kompatibilno sa svim clustering okruženjima podržanim od gore navedenih Exchange Servera	da		
5.3	Central Administration	Softwareom za zaštitu Exchange servera mora se upravljati/pratiti/podešavati na centralnom nivou, preko iste konzole koja se koristi za zaštitu krajnjih točaka	da		
5.4	Antimalware Protection	Software za zaštitu Exchange servera mora integrirati detekciju i dezinfekciju na svim nivoima (mailbox level, transit level) gdje god je to primjenjivo	da		
5.5	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu tako i on-demand detekciju i dezinfekciju svih vrsta prijetnji npr . Viruses, Worms, Trojans, Spyware, Malware, Adware, Hacking Tools, Cryptolocker, itd	da		
5.6	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu tako i on-demand detekciju prijetnji u zapakiranim arhivima (npr zip, rar , cab itd)	da		
5.6	Anti-spam Protection	Rješenje mora ponuditi filtriranje spam-a u realnom vremenu , tako da se blokiraju neželjeni e-mailovi	da		
5.6.1	Anti-spam Protection	Rješenje mora omogućiti kreiranje crnih i bijelih lista.	da		
5.6.2	Anti-spam Protection	Rješenje mora omogućiti definiranje akcije koja će biti poduzeta kada se detektira spam (flag, delete, redirect itd.)	da		

	KARAKTERISTIKE		ZAHTJEV	ODGOVOR da/ne	
6.	Technical Specifications of advanced protection EDR – Endpoint Detection&Response				
6.1	Centralized Event monitoring	Rješenje mora imati long-term fokus na napad, detekciju i dinamičko blokiranje alata, taktika, tehnika i zlonamjernih procedura (TPPs)			
6.2	Centralized Event monitoring	Rješenje mora ponuditi automatsku klasifikaciju SVIH pokrenutih aplikacija i servisa kao goodware i malware, known i unknown u realnom vremenu	da		
6.3	Centralized Event monitoring	Rješenje mora ponuditi više nivoa monitoringa SVIH pokrenutih aplikacija i servisa u realnom vremenu	da		
6.4	Centralized Event monitoring	Rješenje mora omogućiti rekvalifikaciju pokrenutih aplikacija koje su kvalificirane kao malware, unknown, known	da		
6.5	Centralized Event monitoring	Rješenje mora ponuditi tracking izvršenih akcija aplikacija klasificiranih kao malware, tj detaljnu forenzičnu analizu izvršenih akcija prepoznatih kao malware, timelin	da		
6.6	Centralized Event monitoring	Automatska klasifikacija pokrenutih aplikacija na svim endpoint agentima korištenjem learning technique classification data platform	da		
6.7	Centralized Event monitoring	Mogućnost ručne klasifikacije pokrenutih aplikacija na svim endpointima	da		
6.8	Centralized Event monitoring	Monitoring u realnom vremenu u grafičko tabelarnom prikazu kako je došlo do pokretanja malwarea	da		
6.9	Incident investigation tools	Rješenje mora omogućiti timeline napada (files, records, drivers etc.) i njihov utjecaj (e.g. napadnuti resursi, zombi računala ili uređaji)	da		
6.10	Incident investigation tools	Rješenje mora pružiti informacije u realnom vremenu o aktivnostima "napadača": origin, cause, impacted assets and actions taken	da		
6.11	Application control	Rješenje mora ponuditi automatsku provjeru i klasifikaciju SVIH pokrenutih aplikacija i servisa u realnom vremenu	da		
6.12	Application control	Rješenje mora ponuditi automatsku blokadu i klasifikaciju SVIH pokrenutih aplikacija i servisa koji nisu prepoznati kao goodware	da		
6.13	Integration	Rješenje mora imati mogućnost pune integracije sa drugim alatima za analizu, a naročito SIEM	da		

	KARAKTERISTIKE		ZAHTJEV	ODGOVOR da/ne	
7.	Technical Specifications of Antimalware Mail Software For SMTP Server Platforms				
7.1	Supported SMTP server	Ponuđeno rješenje mora biti kompatibilno sa svim SMTP mail serverima u proxy modu. Rješenje mora biti podržano za Windows 2008r2, 2012r2 I 2016, 64 -bitna podrška I Ubuntu server distribucije.	da		
7.2	Supported Environments	Ponuđeno rješenje mora biti u potpunosti kompatibilno sa svim clustering okruženjima podržanim od gore navedenih Servera	da		
7.3	Central Administration	Softwareom za zaštitu SMTP servera mora se upravljati/pratiti/podešavati na centralnom nivou, preko iste konzole koja se koristi za zaštitu krajnjih točaka	da		
7.4	Antimalware Protection	Software za zaštitu SMTP servera mora integrirati detekciju i dezinfekciju na svim nivoima (mailbox level, transit level) gdje god je to primjenjivo	da		
7.5	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu tako i on-demand detekciju i dezinfekciju svih vrsta prijetnji npr . Viruses, Worms, Trojans, Spyware, Malware, Adware, Hacking Tools, Cryptolocker, itd	da		
7.6	Antimalware Protection	Rješenje mora ponuditi kako u realnom vremenu tako i on-demand detekciju prijetnji u zapakiranim arhivima (npr zip, rar , cab itd)	da		
7.6	Anti-spam Protection	Rješenje mora ponuditi filtriranje spam-a u realnom vremenu , tako da se blokiraju neželjeni e-mailovi	da		
7.6.1	Anti-spam Protection	Rješenje mora omogućiti kreiranje crnih i bijelih lista.	da		
7.6.2	Anti-spam Protection	Rješenje mora omogućiti definiranje akcije koja će biti poduzeta kada se detektira spam (flag, delete, redirect itd.)	da		

	KARAKTERISTIKE		ZAHTJEV	ODGOVOR da/ne	
8.	Tehnička specifikacija za Patch management				
8.1.1	Solution	Patch menadžment konzola za software mora biti web-based	da		
8.1.2	Solution (Specify version & release date)	Pristup patch menadžment konzoli treba se obavljati preko SSL protokola	da		
8.1.3	Solution	Patch menadžment konzola mora biti integrirana u jedinstveno web menadžment rješenje s AV-om.	da		
8.1.4	Licensing	Patch menadžment licenca za 350 radnih i serverskih stanica (device).	da		

8.2..1	Solution	Patch menadžment konzola mora imati mogućnost definiranja različitih prava za korisnike koji su kreirani (npr. Monitoring, Basic Administration, Total Control itd)	da		
8.2.2	Solution (Specify version & release date)	Software za upravljanje mora podržavati napredno podešavanje za update, da update / upgrade / downgrade se može provoditi u određenim intervalima ili u određeno vrijeme .	da		
8.3	Agent based deployment	Rješenje za upravljanje mora podržavati instalaciju, kompletnu administraciju i praćenje klijentskog softwarea preko agenta ili modula za upravljanje koji je nezavisan od softwarea za zaštitu klijenta.	da		
8.4	Remote Agent installation	Agent ili modul za upravljanje mora podržavati daljinsku instalaciju	da		
8.5	Manual Agent installation	Agent ili modul za upravljanje mora podržavati ručnu instalaciju	da		
8.6	Centralized Administration	Platforma mora biti u stanju da centralno upravlja svim klijentima na kojima su agenti (monitoring statusa klijenta, obavlja nadogradnji i sl.) u intranet i internet okruženju	da		
8.7	Multiple Configurations support	Platforma mora omogućiti više konfiguracija i podršku grupama na koje oni će konfiguracije biti primenjene	da		
8.8	Profile Support	Platforma mora podržavati profile tako da omogući različite nivoe pristupa za administrativno osoblje	da		

Potpis i pečat ponuditelja