Izmjena postupka

OSNOVNI PODACI

Opis predmeta javne nabavke:

Instaliranje meil servera Državnog tužilaštva, novi domen server i wsus server

Vrsta predmeta:

Robe

Vrsta postupka:

Otvoreni postupak

PODACI O NARUČIOCU

Naziv:

SEKRETARIJAT TUŽILAČKOG SAVJETA

PIB:

11002161

Uslovi prije izmjena

Opis	Tip uslova
Ponuđač je dužan dostaviti bezuslovnu i na prvi poziv naplativu garanciju ponude u iznosu od 2 % procijenjene vrijednosti javne nabavke, kao garanciju ostajanja u obavezi prema ponudi u periodu važenja ponude i 7 dana nakon isteka važenja ponude.	Garancija ponude

U postupku javne nabavke može da učestvuje samo privredni subjekat koji: 1) nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu što se dokazuje na osnovu uvjerenja, potvrde ili drugog akta nadležnog organa izdato na osnovu kaznene evidencije, u skladu sa propisima države u kojoj privredni subjekat ima sjedište, odnosno u kojoj ovlašćeno lice tog privrednog subjekta ima prebivalište	Obavezni uslovi
U postupku javne nabavke može da učestvuje samo privredni subjekat koji je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje što se dokazuje na osnovu uvjerenja, potvrd3 ili drugog akta koji izdaje organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište	Obavezni uslovi
Izjava privrednog subjekta	ESPD
Izjava ponuđača da je cijelokupna oprema nova i nekorišćena.	Drugi uslovi
Ponuđač je u obavezi da dostavi dokaz da je (ukoliko nije proizvođač) u partnerskom odnosu sa proizvođačem za stavke 1-8, što se dokazuje autorizacijom proizvođača od strane proizvođača "MAF"(eng. Manufacturer's Autorization Form) kao i potvrdom proizvođača predmetne opreme “MAF” sa informacijom da je ovlašćen da nudi isporuči i održava opremu i softver koja je predmet javne nabavke. U slučaju da Ponuđač nije zastupnik proizvođača, već da nabavku vrši preko druge kompanije koja je zastupnik proizvođača, u tom slučaju Ponuđač je u obavezi da dostavi ovjerenu kopiju važećeg ugovora/ovlašćenja sa kompanijom koja je zastupnik proizvođača, dok za kompaniju koja je ovlašćeni zastupnik proizvođača treba da bude dostavljen MAF.	Drugi uslovi

Rok izvršenja ugovora (Rok isporuke): ne može biti biti duži od 120 kalendarskih dana od dana zaključivanja ugovora.	Rok izvršenja ugovora
mjesto izvršenja ugovora Podgorica	Mjesto izvršenja ugovora
način plaćanja - virmanski	Način plaćanja
rok plaćanja - 30 dana od uspješno izvršene isporuke	Rok plaćanja
rok važenja ponude - 60 dana od dana javnog otvaranja	Rok važenja ponude

Uslovi nakon izmjena

Opis	Tip uslova
Ponuđač je dužan dostaviti bezuslovnu i na prvi poziv naplativu garanciju ponude u iznosu od 2 % procijenjene vrijednosti javne nabavke, kao garanciju ostajanja u obavezi prema ponudi u periodu važenja ponude i 7 dana nakon isteka važenja ponude.	Garancija ponude
U postupku javne nabavke može da učestvuje samo privredni subjekat koji: 1) nije pravosnažno osuđivan i čiji izvršni direktor nije pravosnažno osuđivan za neko od krivičnih djela sa obilježjima: a) kriminalnog udruživanja; b) stvaranja kriminalne organizacije; c) davanje mita; č) primanje mita; ć) davanje mita u privrednom poslovanju; d) primanje mita u privrednom poslovanju; dž) utaja poreza i doprinosa; đ) prevare; e) terorizma; f) finansiranja terorizma; g) terorističkog udruživanja; h) učestovanja u stranim oružanim formacijama; i) pranja novca; j) trgovine ljudima; k) trgovine maloljetnim licima radi usvojenja; l) zasnivanja ropskog odnosa i prevoza lica u ropskom odnosu što se dokazuje na osnovu uvjerenja, potvrde ili drugog akta nadležnog organa izdato na osnovu kaznene evidencije, u skladu sa propisima države u kojoj privredni subjekat ima sjedište, odnosno u kojoj ovlašćeno lice tog privrednog subjekta ima prebivalište	Obavezni uslovi

U postupku javne nabavke može da učestvuje samo privredni subjekat koji je izmirio sve dospjele obaveze po osnovu poreza i doprinosa za penzijsko i zdravstveno osiguranje što se dokazuje na osnovu uvjerenja, potvrd3 ili drugog akta koji izdaje organ uprave nadležan za naplatu poreskih prihoda, odnosno nadležni organ države u kojoj privredni subjekat ima sjedište	Obavezni uslovi
Izjava privrednog subjekta	ESPD
Izjava ponuđača da je cijelokupna oprema nova i nekorišćena.	Drugi uslovi
Ponuđač je u obavezi da dostavi dokaz da je (ukoliko nije proizvođač) u partnerskom odnosu sa proizvođačem za stavke 1-10, što se dokazuje autorizacijom proizvođača od strane proizvođača "MAF"(eng. Manufacturer's Autorization Form) kao i potvrdom proizvođača predmetne opreme “MAF” sa informacijom da je ovlašćen da nudi isporuči i održava opremu i softver koja je predmet javne nabavke. U slučaju da Ponuđač nije zastupnik proizvođača, već da nabavku vrši preko druge kompanije koja je zastupnik proizvođača, u tom slučaju Ponuđač je u obavezi da dostavi ovjerenu kopiju važećeg ugovora/ovlašćenja sa kompanijom koja je zastupnik proizvođača, dok za kompaniju koja je ovlašćeni zastupnik proizvođača treba da bude dostavljen MAF.	Drugi uslovi
Rok izvršenja ugovora (Rok isporuke): ne može biti biti duži od 120 kalendarskih dana od dana zaključivanja ugovora.	Rok izvršenja ugovora
mjesto izvršenja ugovora Podgorica	Mjesto izvršenja ugovora
način plaćanja - virmanski	Način plaćanja
rok plaćanja - 30 dana od uspješno izvršene isporuke	Rok plaćanja
rok važenja ponude - 60 dana od dana javnog otvaranja	Rok važenja ponude

Kriterijumi prije izmjena

Opis	Očekivani odgovor ponuđača	Metod bodovanja
Cijena	-	-
Rok izvršenja ugovora (Rok isporuke): ne može biti biti duži od 120 kalendarskih dana od dana zaključivanja ugovora.	Eksplicitna numerička vrijednost	Relativno

Kriterijumi nakon izmjena

Opis	Očekivani odgovor ponuđača	Metod bodovanja
Cijena	-	-
Rok izvršenja ugovora (Rok isporuke): ne može biti biti duži od 120 kalendarskih dana od dana zaključivanja ugovora.	Eksplicitna numerička vrijednost	Relativno

Tehnička specifikacija prije izmjena

Procijenjena vrijednost bez PDV	Redni broj predmeta nabavke	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina	Jedinica mjere
99174.00	1	Server za virtualizaciju	Nabavka, isporuka i instalacija servera i platforme za virtuelizaciju. Server - Minimalno sledećih karakteristika: Rack server 1U. Procesor: minimum 2 x CPU 2.4 GHz (turbo frekvencija 3.4 GHz), 16 jezgara, 32 niti, 24 MB cache Memorija: minimalno 256 GB DDR4-3200 RDIM, podržano 2 TB memorije, server mora imati 32 memorijska slota. Storage Controller sa 8 GB FBWC (RAID 0/1/10/5/50/6/60) sa baterijom Disk: minimalno 2 x 480 GB SSD Mixed Use Hot Plug. Server mora da ima prostora za 8xSFF Mreža: minimum 6 x 1Gb Ethernet portova, minimum 1 x management port, 2 x 10 GbE SFP+, 1x 32Gb Dual Port Fibre Channel Host Bus Adapter USB: min 3 PCIe: min 3 PCIe slots x16	2.00	kom

			Napajanje: 2 x 800 W Hot Plug Power Supply Bezbjednost: kriptografski firmware potpis, sistem za prevenciju instalacije „root kit“ prilikom podizanja sistema, bespovratno brisanje podataka sa diskova, Silicon Root of Trust (onemogućavanje ubacivanja malware, virusa ili koda koji može uticati na boot proces servera), sistem za onemogućavanje nenamjernih izmjena nakon inicijalne konfiguracije), TPM 2.0 Administracija: lokalna i daljinska, uključuje napredne funkcije kao što su: directory services (AD, LDAP), dvofaktorska autentifikacija, single singn-on, PK autentifikacija, virtuelni folderi, daljinski file share, VNC veza sa operativnim sistemom, vitruelna konzola, kontrola snage (postavljanje granica i upozorenja), daljinsko instaliranje operativnog sistema Komplet šina za jednostavno postavljanje u rek i cable management Garancija: proizvođačka garancija minimum 3 godine Platforma za virtualizaciju: VMware vSphere Essentials Plus Kit 3 hosts (max 2 CPU/host,max 32 cores/CPU socket) [VMware Software - [DSVQUIK]] (210-AIKY) Components 1 487-15781 3 Years ProSupport VMware vSphere 8 Essentials Plus Kit for 3 Hosts Sftwr Spt-Maint (ZR) Software 1 528-CUXR VMware vSphere 8 Ess Plus Kit for 3 hosts (Max 2 CPU per host, 32 cores/CPU),3YR Vmware SNS (ZR)		
	2	Storidž sistem	Nabavka, isporuka i instalacija storidž sistema minimalno sledećih karakteristika: Storidž sistem mora da podržava minimum 24 x 2.5” hot-plug diska po enkložeru; podržava ukupno 272 diska uz dodatne enkložere potrebno je da podržava enkložere koji prihvataju do 84 x 3.5” diskova sa pojedinačnim kapacitetima do 20 TB storidž RAID controller, sa podrškom za: SSD, SAS i NLSAS diskove; RAID 1, 5, 6, 10, kao i distribuirani tip RAID koji kreira distribuirani rezervni (spare)	1.00	kom

		prostor i na taj način omogućava aktivno korišćenje svih diskova sve vrijeme i ubrzava rebuild operacije tražena konfiguracija treba da ima minimum 8 x min 1.92TB SSD hot plug; Optimizacija: auto-tiering (do 3 primarna), Thin Provisioning , 1024 snapshota Mobilnost i migracija: asinhrona replikacija (jedan-na-više ili više-na-jedan), kopiranje kompletnih volume-a storidž je potrebno da ima redundantne kontrolere sa po minimum 4 (32 Gb FC) porta koji će omogućiti redundantnu konekciju servera; minimalno 16 GB memorije po kontroleru 2 management porta minimum 4 FC modula 32 Gb short wave FC transivera kompatibilnih sa ponuđenim storidžom; Form factor - 2U; Napajanje minimalno 550 W, redundantno Uz ponuđenu opremu je potrebno isporučiti i softver za nadgledanje servera i storage koji može pratiti inventar uređaja, aktivno stanje i alarmne situacije Garancija: proizvođačka garancija minimum 3 godine		
3	Uređaj za skladištenje rezervnih kopija podataka	Nabavka, isporuka i instalacija uređaja za skladištenje rezervnih kopija podataka minimalno sledećih karakteristika: Rack server maximalno 2U. Procesor: minimum 1 x CPU 2.2 GHz (turbo frekvencija 2.7 GHz), 6 jezgara, 12 niti, 9 MB cache Memorija: minimalno 8 GB DDR4, podržano 64 GB memorije, server mora imati 4 memorijska slota. Storage Controller broj slotova mimum 12 2.5 ili 3.5 Disk: minimalno 6 x 8 TB SATA Hot Plug. Mreža: minimum 4 x 1Gb Ethernet portova, USB:minimalno 2 PCIe: minimalno 2 PCIe slots x8 Napajanje: 2 x 500 W Hot Plug Power Supply Uključene šine za rack. Garancija: proizvođačka garancija minimum 2 godine	1.00	kom

4	Backup platforma	Bekap rješenje mora da zadovoljava sljedeće kriterijume: Mora da podržava mogućnost instalacije na Windows OS, Linux OS, NAS. Mogućnost inastalacije kao virtuelni apliance ili Amazon machine image za AWS Mogucnost VMware i Hyper-V backup Funkcionalnosti minimalno za VMware: • zaštita podataka za vCentar i ESXi • mogućnost kreiranja sigurnosnih kopija bez agenta • trenutni recovery VM-ova, datoteka i objekata aplikacija • kopiranje VMware VM sigurnosne kopije van primarne lokacije, na traku ili pohranu u cloud • Automatsko testiranje sigurnosne kopije kako bi se provjerilo da li se podaci mogu oporaviti • Automatska zaštita preko polisa kako bi se uštedjelo vrijeme Funkcionalnosti minimalno za Hyper-V: • mogućnost kreiranja sigurnosnih kopija bez agenta • trenutni granularni recovery • trenutni oporavak datoteka i objekata aplikacija direktno iz kompresovanih rezervnih kopija sa očuvanim svim dozvolama • Automatsko testiranje sigurnosne kopije kako bi se provjerilo da li se podaci mogu oporaviti • Automatska zaštita pomoću polisa, skripti i APIa Licenca i tehnička podrška u trajanju od minimum tri godine (36 mjeseci).	1.00	kom
5	Security platforma za zaštitu email saobraćaja - Nabavka, isporuka i instalacija email antispam rješenja	Barracuda Email Security Gateway ili ekvivalent Minimalne karakteristike: Email Security Gateway mora da ima mogućnost filtriranja dolaznih poruke emailova i zaštitu email serverae od neželjenih i lažnih eemail poruka koji obuhvataju sledeće: neželjeni emailovi, zlonamjernog softvera, krađe identiteta, otkrivanja informacija, curenja podataka. Email Security Gateway mora da ima mogućnost filtriranja odlaznih emailova od neželjenih emailova i nepoželjnog sadržaja	1.00	kom

kako bi zaštitio reputaciju IP adresa i domena emailova i izbjegao unose na javne crne liste/liste odbijanja/liste blokiranja.
Email Security Gateway mora da ima mogućnost da prima dolazne emailove preko SMTP, IMAP i POP protokola. Email Security Gateway mora da ima mogućnost da prosljeđuje dolazne i odlazne emailove preko SMTP protokola.
Email Security Gateway mora da ima mogućnost da se konfiguriše pomoću Web korisničkim interfejsom. Email Security Gateway mora da ima mogućnost da podržava više domena. Virtuelna mašina Email Security Gateway mora da ima mogućnost da ima licencu za najmanje 2 virtuelna CPU-a.
Filtriranje dolaznih emailova Filtriranje neželjenih mailova (Spam filtering) mora da ima sledeće mogućnosti: Klasifikacija neželjenih emailova mora da bude automatska i da funkcioniše bez potrebe za konfiguracijom ili finim podešavanjem. Klasifikacija neželjenih emailova mora da se zasniva na analizi namjere. Klasifikacija neželjenih emailova mora da se zasniva na traženju baze podataka o poznatim neželjenim prijetnjama (eng. Known-spam fingerprint database lookup). Klasifikacija neželjenih emailova mora da se zasniva na analizi slike sa optičkim prepoznavanjem znakova. Klasifikacija neželjenih emailova mora da podržava Bayesian mehanizam analize. Emailovi moraju da imaju mogućnost podešavanja spam ocjene (eng. Spam score). Administrator mora da ima mogućnost da mapira nivoe vjerovatnoće neželjenih mailova i sprovede odgovarajuće akcije; u zavisnosti od konfigurisanog nivoa vjerovatnoće, poruke treba da se obrađuju u četiri nivoa: prihvaćeni emailovi, označeni emailovi, emailovi u karantinu, blokirani emailovi. Tekst za označavanje emailova mora da ima mogucnost da se konfiguriše.
Zaštita od zlonamjernog softvera (malware) mora da ima sledeće mogućnosti: Svi dolazni emailovi i prilozi moraju da se skeniraju sa najmanje tri nezavisna antivirusna mehanizma. Filtriranje zasnovano na reputaciji (Reputation-based filtering) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima bazu podataka reputacije IP adresa sa opcijom za

blokiranje, karantin, označavanje ili onemogućavanje. Email Security Gateway mora da ima klasifikaciju emailova masovnog slanja da bi se prepoznali emailovi sa mailing liste, emailovi društvenih medija, marketinški emailovi sa opcijama za blokiranje, karantin, označavanje ili onemogućavanje. Email Security Gateway mora da ima integraciju sa Blok listama eksterne reputacije (External RBL).
Filtriranje zasnovano na kontroli brzine (Rate control filtering) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost definisanja maksimalanog broja dolaznih konekcija po IP adresi u vremenskom period.
Filtriranje pošiljaoca za dolazni email saobraćaj (Filtering of senders for inbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost stavljanja adrese emaila ili domena emaila na bijelu listu. Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja email adrese ili domena određenog pošiljaoca. Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja emailova u slučaju neuspjele verifikacije SPF-a (Sender's Policy Framework). Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja emailova u slučaju neuspjele DKIM verifikacije (Domain Keys Identified Mail). Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja emailova koji dolaze sa IP adresa bez DNS PTR zapisa (reverse DNS verification). Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja emailova koji dolaze sa DNS domena specifičnih za državu ili domena najvišeg nivoa (npr. *.cn za Kinu). Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja emailova skupovima karaktera specifičnim za odabrane jezike.
Filtriranje primalaca za dolazne emailove (Filtering of recipients for inbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost stavljanja adrese emaila ili domena primaoca na bijelu listu. Email Security

Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja email adrese ili domena određenog primaoca. Filtriranje priloga za dolazne emailove (Filtering of attachments for inbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost blokiranja ili stavljanja u karantin emailova prema imenu priloga ili obrascu imena. Email Security Gateway mora da ima mogućnost blokiranja ili stavljanja u karantin emailova prema tipu MIME priloga. Email Security Gateway mora da ima mogućnost blokiranja ili stavljanja u karantin emailova prema kategoriji priloga; najmanje sledeće kategorije mora prepoznati: MS-Office dokumenti, PDF dokumenti, izvršne datoteke, multimedijalne datoteke, Windows skripte. Email Security Gateway mora da ima mogućnost blokiranja ili stavljanja u karantin emailova sa prilozima koji sadrže određene ključne riječi ili tekstualne obrasce.

Filtriranje sadržaja mailova (Message content filtering) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin, označavamnja (eng. Tag) emailova sa određenim ključnim riječima ili obrascima u predmetu, zaglavlju ili tijelu email poruke. Odlazno filtriranje Filtriranje neželjene email pošte za odlazni saobraćaj (Spam filtering for outbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost klasifikacije neželjene email pošte koja treba da bude automatska i da funkcioniše bez potrebe za konfiguracijom ili finim podešavanjem. Email Security Gateway mora da ima mogućnost klasifikacije neželjene email pošte koja treba da se zasniva na analizi namjere. Email Security Gateway mora da ima mogućnost klasifikacije neželjene email pošte koja treba da se zasniva na analizi slike sa optičkim prepoznavanjem znakova. Email Security Gateway mora da ima mogućnost da emailovima dodijeljuje vjerovatnoću neželjene email pošte (spam score). Email Security Gateway mora da ima mogućnost da administrator može da mapira nivoe vjerovatnoće neželjene email pošte i u zavisnosti od konfigurisanih nivoa vjerovatnoće, emailovi moraju da budu

obrađeni kao: prihvaćeni emailovi, emailovi u karantinu, blokirani emailovi. Zaštita od zlonamjernog softvera za odlazni email saobraćaj (Malware protection for outbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost da sve odlazne email poruke i priloge skenirati sa tri nezavisna antivirusna mehanizma.
Filtriranje kontrole brzine odlaznog email saobraćaja za zaštitu reputacije i izbjegavanje crne liste (Rate control filtering of outbound traffic for reputation protection and blacklisting avoidance) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost da nametne/defineše maksimalan broj primalaca po pošiljaocu za određeni vremenski period.
Filtriranje primalaca za odlazni email saobraćaj (Filtering of recipients for outbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost preusmjeravanja isporuke na email adrese ili domene na alternativni email server.
Filtriranje priloga za odlazni email saobraćaj (Filtering of attachments for outbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili preusmjeravanja email poruke sa prilozima određenog imena ili šablona imena. Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili preusmjeravanja email poruke prema tipu MIME priloga. Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili preusmjeravanja email poruke prema kategoriji priloga; najmanje sledeće kategorije treba prepoznati: MS-Office dokumenti, PDF dokumenti, izvršne datoteke, multimedijske datoteke, Windows skripte. Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili preusmjeravanja email poruke sa prilozima koji sadrže određene ključne riječi ili tekstualne obrasce.
Filtriranje sadržaja email poruka (Message content filtering) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili preusmjeravanja email poruke sa

određenim ključnim riječima ili obrascima u predmetu, zaglavlju ili tijelu email poruke. Karantin i baferovanje poruka (Quarantine and message buffering) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost omogućavanja karantina po korisniku. Email Security Gateway mora da ima mogućnost omogućavanja email adrese u globalnom karantinu. Email Security Gateway mora da ima mogućnost baferovanja svih dolaznih i odlaznih email poruka i poništavanja odluka o blokiranju za pojedinačne email poruke (čak i blokirane email poruke treba da se mogu vratiti i isporučiti radnjom administratora). Monitoring Email Security Gateway mora da ima ugrađeni monitoring dostupan putem web korisničkog interfejsa i da sadrži najmanje sledece karakteristike: monitoring storidža: iskorišten/slobodan prostor, performanse obrade i slobodni kapacitet, statistika poruka po satu, mogućnost SYSLOG integracija. Izvještavanje Email Security Gateway mora da ima sistem izvještavanja koji je dostupan putem web interfejsa i da sadrži najmanje sledece karakteristike: Planirani i trenutni izvještaji moraju biti dostupni za određene vremenske periode, sveobuhvatan skup izveštaja sa najmanje sledećim karakteristikama: pošiljaoce neželjene pošte, primaoce neželjene pošte, aktivnost virusa, veličine poruka, kršenja SPF-a. Email Security Gateway mora da ima upravljanje korisnicima i da sadrži najmanje sledece karakteristike: LDAP/Active Directory integracija za verifikaciju primaoca emailova, Podrška za LDAP, Radius ili lokalnu bazu podataka za verifikaciju pristupa korisnika za karantin po korisniku i korisničke postavke. Email Security Gateway mora da ima skalabilnost i visoku dostupnost sledećih karakteristika: podrška za grupisanje i federalni pristup baferu poruka (klasterirani uređaji su vidljivi kao jedan izvor podataka kada se poruke sortiraju i/ili oslobađaju od blokiranja), aktivno sa eksternim load-balancer. Email Security Gateway mora da ima mogucnost dnevnika poruka koji podrzumjeva sledeće: podrška za evidentiranje svih dolaznih i odlaznih poruka direktno sa sistema email gateway-a.

Licenca u trajanju od minimum dvije godine (24 mjeseca).
Minimalne karakteristike: Rješenje mora biti kompatibilno sa Check point security gateway-ima.
Centralni management sistem mora da se isporuči u .iso formatu zajedno sa licencom koja omogućava upravljanje nad najmanje 5 firewall uređaja. Model licenciranja mora biti takav da ne sadrži ograničenja po pitanju korištenih resursa (CPU, Memorija, HDD).
Rješenje mora imati mogućnost instalacije na najmanje sljedeće platforme Hyper-V (Windows 2016 Server и Windows 2012 Server R2), KVM (REHL 7 / CentOS 7), VMware vSphere 6.5/6.7) kao i Open server platforme.
Rješenje mora da ima mogućnosti: - Centralizovanog kreiranja bezbjednosnih pravila (eng. security policy) i distribuciju pravila na uređaje -Prikupljanje i čuvanje logova o saobraćaju kroz uređaj,
- Prikupljanje i čuvanje administratorskih logova (eng. audit logs)
- Korelaciju bezbjednosnih logova i prikazivanje izvještaja o statistici saobraćaja koji prolazi kroz uređaj za zaštitu informaciono komunikacione mreže (eng. Event Correlation)
- Rješenje mora da posjeduje mogućnost korelacije bezbjednosnih događaja (eng. Event Correlation).
- Rješenje mora da ima mogućnost grafičkog prikaza bezbjednosnih incidenata u mreži kroz predefinisane profile.
- Rješenje mora da posjeduje mogućnost kreiranja izvještaja o bezbjednosnim incidentima kao i statistici saobraćaja.
- -Rješenje mora da posjeduje predefinisane tipove izvještaja kao i mogućnost kreiranja novih tipova izvještaja shodno zahtjevu i potrebi korisnika.
Rješenje mora da ima mogućnost kreiranja više administratorskih profila, sa različitim privilegijama pri čemu administrator mogu istovremeno da rade na istim bezbjednosnim pravilima bez međusobnog prekidanja rada (promjenu pravila i instalaciju pravila).
Rješenje mora da ima integrisani x.509 CA (eng. certificate authority).
Garancija i tehnička podrška: Dostupnost tehničke podrške proizvođača po principu

		24x7 , Pristup bazi znanja (tehničkoj dokumentaciji) proizvođača, " Pristup bazi znanja (tehničkoj dokumentaciji) proizvođača, Uključena garancija i tehnička podrška u trajanju od minimalno 2 godine (24 mjeseca). U ponudi mora da bude uključen servis ažuriranja svih vrsta prijetnji u trajanju od 2 godine (24 mjeseca)."		
6	Nabavka, isporuka i instalacija Security Management platforme:	Minimalne karakteristike: Rješenje mora biti kompatibilno sa Check point security gateway-ima. Centralni management sistem mora da se isporuči u .iso formatu zajedno sa licencom koja omogućava upravljanje nad najmanje 5 firewall uređaja. Model licenciranja mora biti takav da ne sadrži ograničenja po pitanju korištenih resursa (CPU, Memorija, HDD). Rješenje mora imati mogućnost instalacije na najmanje sljedeće platforme Hyper-V (Windows 2016 Server и Windows 2012 Server R2), KVM (REHL 7 / CentOS 7), VMware vSphere 6.5/6.7) kao i Open server platforme. Rješenje mora da ima mogućnosti: - Centralizovanog kreiranja bezbjednosnih pravila (eng. security policy) i distribuciju pravila na uređaje -Prikupljanje i čuvanje logova o saobraćaju kroz uređaj, - Prikupljanje i čuvanje administratorskih logova (eng. audit logs) - Korelaciju bezbjednosnih logova i prikazivanje izvještaja o statistici saobraćaja koji prolazi kroz uređaj za zaštitu informaciono komunikacione mreže (eng. Event Correlation) - Rješenje mora da posjeduje mogućnost korelacije bezbjednosnih događaja (eng. Event Correlation). - Rješenje mora da ima mogućnost grafičkog prikaza bezbjednosnih incidenata u mreži kroz predefinisane profile. - Rješenje mora da posjeduje mogućnost kreiranja izvještaja o bezbjednosnim incidentima kao i statistici saobraćaja. - -Rješenje mora da posjeduje predefinisane tipove izvještaja kao i mogućnost kreiranja novih tipova izvještaja shodno zahtjevu i potrebi korisnika. Rješenje mora da ima mogućnost kreiranja	1.00	kom

		više administratorskih profila, sa različitim privilegijama pri čemu administrator mogu istovremeno da rade na istim bezbjednosnim pravilima bez međusobnog prekidanja rada (promjenu pravila i instalaciju pravila). Rješenje mora da ima integrisani x.509 CA (eng. certificate authority). Garancija i tehnička podrška: Dostupnost tehničke podrške proizvođača po principu 24x7 , Pristup bazi znanja (tehničkoj dokumentaciji) proizvođača, " Pristup bazi znanja (tehničkoj dokumentaciji) proizvođača, Uključena garancija i tehnička podrška u trajanju od minimalno 2 godine (24 mjeseca). U ponudi mora da bude uključen servis ažuriranja svih vrsta prijetnji u trajanju od 2 godine (24 mjeseca)."		
	7	Nabavka, isporuka i instalacija Security Gateway Sisitema:	MinB33:B71Check point security gateway-ima. Traženo rješenje mora imati mogućnost implementacije u okviru softwerski definisanog datacentra zasnovanog na VmWare ESXI rješenju sa ciljem inspekcije saobraćaja Model licenciranja je zasnovan na broju virtuelnih korova dodijeljenih virtuelnoj mašini koja ga pokreće Tražena licenca 2 procesorska kora Perfomanse: Perfomanse ekvivalentne konfiguraciji 2 x vCore Intel xeon E5-2630 v3 / 8 GB RAM Memory Minimalni firewall throughput 7 Gbps NGFW propusna moć (firewall, application control i IPS) od najmanje 2,7 Gbps Propusna moć (firewall, application control, URL filtering, IPS, Antivirus AntiBoot) od najmanje 0,9 Gbps Firewall + IPS propusna moć od najmanje 3,9 Gbps Rješenje mora podržavati mogućnost rada u Active/Active L2, Active/Passive L2 i L3(routing) režimu rada Rješenje mora imati mogućnost kreiranja dinamičkih pravila (polisa) na osnovu identiteta dobijenih od najmanje sledećih izvora: Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers i 3rd parties uređaja kroz Web API integraciju. Rješenje mora da podržava mogućnost rada u MTA modu OSPFv2 and v3, BGP, RIP i	2.00	kom

Policy-based routing
Rješenje mora da uključuje sledeće bezbednosne servise: Application Control, URL filtering, Content Awareness, IPS, Anti-virus, Anti-Bot, Anti-Spam & Email zaštitu, zero-day zaštitu zasnovanu na cloud based i/ili on-premises SandBox tehnologiji, VPN, Remote Access VPN
Rješenje mora da podržava DLP zaštitu kroz instalaciju dodatne licence bez kupovine dodatne opreme Rješenje mora imati mogućnost zero-day zaštite bazirane na cloud based i/ili on-premises SandBox tehnologiji za pretnje koje dolaze putem: HTTP, HTTPS, FTP, SMTP i SMTP TLS saobraćaja
Rješenje mora imati mogućnost emuliranja izvršnih fajlova, arhiviranih fajlova, dokumenata, JAVA i Flash aplikacija tj. Najmanje sledećih tipova dokumenata: 7z, cab, csv, doc, ocm, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, tgz, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, gz, bz2
Rješenje mora imati mogućnost inspekcije SSL kriptovanog saobraćaja u dolaznom i odlaznom smeru Rješenje mora da ima mogućnost prepoznavanja najmanje 8000 internet aplikacija,
Rješenje mora da ima mogućnost da koristi URL filtering pravila sa ciljem da omogući administratoru granularnu kontrolu https inspekcije (bypass https inspection)
Rješenje mora da ima najmanje 160 predefinisanih URL kategorija
Kroz Content Awareness bezbednosnu zaštitu Rješenje mora da ima mogućnost prepoznavanja i kontrole najmanje sledečih tipova sadržaja koji se šalje odnosno preuzima kroz http & https: * Arhive, * CSV fajlovi, * database fajlova, * document fajlovi, * Executable fajlova, * Media i slike, * Presentation fajlova, * PCI Credit Card brojevi, Anti-Bot zaštita mora da ima mehanizam detekcije i blokiranja pristupa URL stranicama na osnovu reputacije URLa
Anti-Bot zaštita mora da ima mehanizam detekcije i blokiranja pristupa malicioznim domenima na osnovu reputacije domena
Anti-Bot zaštita mora da ima mehanizam detekcije i blokiranja sumnjivog (malicioznog) ponašanja u mreži

Anti-Virus zaštita mora da ima mehanizam detektovanja malicioznih aktivnosti
Anti-Virus zaštita mora da ima mogućnost skeniranja arhiviranih fajlova
Anti-Virus zaštita mora da ima mogućnost blokiranja pristupa malicioznim URL stranicama
Anti-Virus zaštita mora da ima mogućnost skeniranja linkova unutar Email-a
Minimalne funkcionalnosti rješenja koje moraju biti podržane na menadžment softweru u sklopu licenci: Rješenje mora imati mogućnost kreiranja zaštitnih pravila (eng. security policy), prikupljanja, čuvanje i pregleda logova sa svih zaštitnih funkcionalnosti: firewall,, IPS, URL filtering, application controll, Anti Virus i Anti Bot, zero-day zaštita
Konzola za upravljanje mora da ima grafički mehanizam za prikazivanje koliko je puta bezbjednosno pravilo bilo korišćeno (security rule hit counter)
Za potrebe kreiranja bezbjednosnih pravila koristi se klijentska aplikacija koja se instalira na računarima administratora i koja omogućava menadžment svih bezbjednosnih pravila i koja se isporučuje u .exe formatu i koja se može instalirati neograničeno puta.
Rješenje mora imati mehanizam verifikacije sigurnosnih polisa prije instalacije polisa (eng. security policy verification mechanism)
Rješenje mora da imati mogućnost kreiranja revizije sigurnosnih polisa i mogućnost vraćanja na tu reviziju (eng. policy revision control mehanizam)
Rješenje mora imati mogućnost jednostavnog i brzog kreiranja bezbjednosnih pravila korišćenjem mehanizma prevlačenja objekata (eng. drag & drop) u zaštitno pravilo
Rješenje mora imati mogućnost grupisanja bezbjednosnih pravila u slojeve (eng. layers) i kreiranja pod pravila unutar sloja (eng. sub layers)
Rješenje mora imati mogućnost kreiranja više administratorskih korisnika, pri čemu administratori mogu istovremeno da rade na istom bezbednosnom pravilu bez međusobnog prekidanja rada (promenu pravila i instalaciju pravila)
Rješenje mora imati mogućnost kreiranja više administratorskih profila, sa različitim

		privilegijama pri čemu administratori mogu istovremeno da rade na istom bezbjednosnom pravilu bez međusobnog prekidanja rada (promenu pravila i instalaciju pravila). Rješenje mora da ima mogućnost kreiranja administratorskih korisnika zavisno od njihove uloge. Npr. administratori koji imaju samo mogućnost praćenja: logova, URL pravila, IPS pravila... Rešenje mora imati integrisan interni x.509 CA (eng. certificate authority) softwerski zahtjevi i performanse security menadžment uređaja Garancija i tehnička podrška: - Dostupnost tehničke podrške proizvođača po principu 24x7 - Pristup bazi znanja (tehničkoj dokumentaciji) proizvođača, - Uključena garancija i tehnička podrška u trajanju od minimalno 2 godine (24 mjeseca). U ponudi mora da bude uključen servis ažuriranja svih vrsta prijetnji u trajanju od 2 godine (24 mjeseca).		
8	Sistem za zaštitu Web saobraćaja (WAF)	WebB72:B83odine (36 mjeseci) FortiWeb-VM (1 CPU) FC1-10-WBVMS-582-02-36 ili ekvivalent Ponuđeno rješenje mora da obezbjedi minimalno sledeće tehničke zahteve: Podrška za višenivovsku zaštitu Web aplikacija i API-ja od napada koji s koriste otkrivene i neotkrivene propuste na Webu, Uređaj mora da koristi napredne tehnike mašinskog učenja (na bazi veštačke inteligencije – AI) kako bi modelovao ponašanje svake aplikacije i uočio zlonamerne anomalije i blokirao ih, Uređaj mora da koristi tehnike zaštite kao što su: signature napada, IP adrese reputacija, provera protokola, IP adrese geo-lokacija, cross-site scripting, SQL injection i session hijacking, Uređaj mora da ima mogućnost povezivanja u jedinstvenu sigurnosnu arhitekturu sa firewall uređajima i sandbox sistemima, kako bi se omogućila razmjena sigurnosnih informacija i dublje skeniranje sumljivih fajlova, Podrška za zaštitu od OWASP Top 10 aplikacionih napada (Open Web Application Security Project 10 najkritičnijih rizika),	1.00	kom

Podrška za zaštitu API-ja (Application Programming Interface) i to: usklađenost XML i JSON protokola, API gateway i Web signature,
Podrška za funkcionalnosti bot oslabljivanja i to: detekcija na bazi graničnih vrjednosti, detekciju biometrijskih bot-ova i poznatih bot-ova,
Podrška za sledeće modove implementacije: reverse proxy, inline transparent i offline sniffing,
Podrška za WCCP ili ekvivalentan protokol,
Podrška za zaštitne mehanizme: SQL injection, Man-in-the-Browser, malware detekcija, validacija protokola, white listing, black listing, brute force zaštita, cookie signature i enkripcija, HTTP Header sigurnost, DOS sprečavanje, zaštita od poznatih i zero-day napada, zaštita od „curenja“ podataka (DLP),
Mogućnost za rutiranje na osnovu sadržaja, HTTPS/SSL offloading, HTTP kompresiju, Layer 7 server load balancing, URL rewriting i keširanje,
Podrška za upravljanje kroz grafički Web komandni intefejs, SNMP, Syslog, email logging, REST API i administrativne domene sa različitim ulogama administratora,
Podrška za aktivnu i pasivnu autentifikaciju, Single Sign On (SSO), LDAP, RADIUS i SAML, SSL klijentske sertifikate i CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart),
Podrška za detaljnu grafičku analizu i izveštavanje u vidu ključnih elemenata: aktivnosti korisnika, IP konfiguracije, log zapisi napada i saobraćaja, mape napada i OWASP Top 10 kategorizaciju napada,
Grafička analiza i izveštavanje mora da obezbede administratorima mreže informacije u realnom vremenu koje se odnose na izvor pretnje, koji je rizik za klijente i uređaje i uobičajene prekršaje, kako bi brzo identifikovali sumnjivu aktivnost,

Podrška za opšte funkcionalnosti: IPv6, PKI integracija, čarobnjak (wizard) za podešavanje uobičajenih aplikacija i baza podataka, WebSocket i automatsko konfigurisanje kako bi se pojednostavila implementacija,
Podrška za antivirusnom zaštitom koja skenira sve upload-ovane fajlove koji mogu

		inficirati servere ili druge elemente u mreži, Podrška za Web sigurnosni servis koji sadrži sumnjive URL šablone, signature na aplikativnom nivou, maliciozne robote, skener za update-e na Web ranjivosti (vulnerabilities) i modele prijetnji bazirane na mašinskom učenju, Podrška za servis IP reputacije koji štiti od poznatih izvora napada kao što su spammer-i, anonimni proxy-i i botnet-ovi, Mogućnost za servis zaštite kredencijala koji proverava da li se pokušaj pristupa (logovanja) nalazi na listi kompromitovanih kredencijala i preduzimanje akcija počevši od alarma do blokiranja pristupa za kredencijale (korisničko ime i lozinka) za koje se sumnja da su ukradeni, Propusnost za HTTP saobraćaj: minimalno 25 Mb/s, Propusnost za HTTPS saobraćaj: minimalno 10 Mb/s, Podrška za minimalno 4 administrativna domena, Podrška za povezivanje više uređaja u konfiguraciju visoke dostupnosti, Uključena podrška za neograničeni broj aplikacija ili uključene licence koje to omogućavaju (ukoliko sistem koristi licenciranje za aplikacije), Podrška za instalaciju na sledećem hardverskom sistemu: minimalno 1 vCPU i 8 GB memorije. Podrška za instalaciju na hipevizor i cloud sistemima: VMware, Microsoft Hyper-V, KVM, Citrix XenServer, Microsoft Azure, Google Cloud, Oracle Cloud, i Amazon Web Services Uključena licenca za minimalno 3 godine koja omogućava minimalno sledeće funkcionalnosti: Web sigurnosni servis, servis IP reputacije, zaštita od malware-a, sandbox cloud servis, servis zaštite kredencijala i analitika pretnji, Mora biti uključena u cijenu trogodišnja tehnička podrška proizvođača po modelu 24x7.		
9	Sistem za centralizovano prikupljanje logova, analizu i reporting	PonB104:B120e: Rješenje mora biti kompatibilno sa Fortigate uređajima. Podrška za prikupljanje logova, analitiku i izveštavanje za firewall uređaj Fortinet FortiGate tako da kompatibilnost mora biti potvrđena u dokumentaciji proizvođača	1.00	kom

firewall uređaja,
Podrška za korelaciju događaja i detekciju u realnom vremenu za sve prikupljene logove,
Podrška za dublju vidljivost i kritične mrežne vidljivosti kroz integraciju sa firewall uređajem FortiGate i sa sistemom za zaštitu Web saobraćaja
Podrška za reagovanje u realnom vremenu na napade na mrežu, ranjivosti i upozorenje na potencijalna ugrožavanja, sa inteligencijom za pretnje, korelacijom događaja, nadgledanje, alarme i izvještavanje za trenutni taktički odgovor i oporavak,
Podrška za automatizaciju kako bi odgovorilo na kritične alarme, događaje i SLA parametre (Service Level Agreement) za potrebe usaglašenosti sa regulativnom (compliance),
Podrška za minimum 60 šablona izveštaja (report-a) i minimum 2.000 kombinovanih setova podataka, grafičkih dijagrama i makroa,
Podrška za minimum sledeće formate report-a: CSV, PDF, HTML, JSON i XML,
Podrška za servis indikatora kompromitovanosti sa minimalno 400.000 indikatora dnevno, koji u kombinaciji sa analitikom omogućavaju identifikovanje sumnjivih aktivnosti u mreži ili operativnom sistemu,
Podrška za servis automatizacije sigurnosti koji se oslanja na skriptove, konektore i REST API kako bi se ubrzao odgovor na sigurnosne izazove i smanjilo vreme detekcije,
Podrška za servis detekcije proboja sigurnosti (outbreak) koji sadrži pakete sadržaja kreiranih u realnom vremenu, kako bi se zaštitila mreža na nove malware proboje oktivene od strane globalne inteligencije za prijetnje. Paketi sadržaja mora da sadrže izvještaje, šablone izvještaja i akcije na događaje,
Podrška za minimum 5 GB logova dnevno – centralno logovanje i analitika,
Podrška za instalaciju na sledećem hardverskom sistemu: minimalno 4 vCPU i 8 GB memorije.
Podrška za instalaciju na sa hipevizor i cloud sistemima: VMware, Microsoft Hyper-V, KVM, Citrix XenServer, Microsoft Azure, Google Cloud, Oracle Cloud, i Amazon Web

			Services Uključena licenca za minimalno 3 godine koja omogućava minimalno sledeće funkcionalnosti: servis indikatora kompromitovanosti, servis automatizacije sigurnosti i servis detekcije proboja sigurnosti (outbreak), Mora biti uključena u cijenu trogodišnja tehnička podrška proizvođača po modelu 24x7.		
	10	Uredjaj za neprekidno napajanje	Minimalne karakteristike: Tehnologija: Online double conversion Ulazni Priključak: socket IEC60320 C20 Ulazni Napon: 210-240 V Izlazni Priključci: 8 x IEC60320 C13, max. 10A per socket; 1 x IEC60320 C19, max. 16A per socket Snaga: 3000 VA Efikasnist: online 93 % ECO mode efikasnost: 98 %. Izmjenjive baterije u toku rada Kapacitet baterije: 6 x 12V x 9.0 Ah Punjenje baterije: Maximalno 4 časa do 90% kapaciteta nakon potpunog pražnjenja Mogućnost opcionog network menadžmenta Potrovi: USB, RS-232 Maksimalna temperatura rada: 0 - 40 °C Relativna vlažnost: 20 - 90% Maksimalne Dimenzije:19" 2RU Maksimalna težina:28 kg Bezbjedonosni standardi sertifikati: IEC/EN62040-1,IEC/EN60950-1 Elektromagnetni standardni sertifikati: IEC/EN62040-2,IEC61000-4-2,IEC61000-4-3,IEC61000-4-4, IEC61000-4-5,IEC61000-4-6,IEC61000-4-8 CE declaration Rek 19" UPS montažni kit (šine za rek ormar) Garancija: proizvođačka garancija minimum 2 godine	2.00	kom
	11	Usluga instalacije i konfiguracije	Usluge instalacije i konfigurisanja serverske i storadže opreme, kao i instalacija i konfiguracija ponuđenih rješenja i puštanje u operativan i funkcionalan rad. Integracija sa postojecom infrastrukturom u skladu sa zahtjevima i potrebama naručioca.	1.00	kom

Tehnička specifikacija nakon izmjena

Procijenjena vrijednost bez PDV	Redni broj predmeta nabavke	Opis predmeta nabavke	Bitne karakteristike predmeta nabavke	Količina	Jedinica mjere
99174.00	1	Server za virtualizaciju	Nabavka, isporuka i instalacija servera i platforme za virtuelizaciju. Server - Minimalno sledećih karakteristika: Rack server 1U. Procesor: minimum 2 x CPU 2.4 GHz (turbo frekvencija 3.4 GHz), 16 jezgara, 32 niti, 24 MB cache Memorija: minimalno 256 GB DDR4-3200 RDIM, podržano 2 TB memorije, server mora imati 32 memorijska slota. Storage Controller sa 8 GB FBWC (RAID 0/1/10/5/50/6/60) sa baterijom Disk: minimalno 2 x 480 GB SSD Mixed Use Hot Plug. Server mora da ima prostora za 8xSFF Mreža: minimum 6 x 1Gb Ethernet portova, minimum 1 x management port, 2 x 10 GbE SFP+, 1x 32Gb Dual Port Fibre Channel Host Bus Adapter USB: min 3 PCIe: min 3 PCIe slots x16 Napajanje: 2 x 800 W Hot Plug Power Supply Bezbjednost: kriptografski firmware potpis, sistem za prevenciju instalacije „root kit“ prilikom podizanja sistema, bespovratno brisanje podataka sa diskova, Silicon Root of Trust (onemogućavanje ubacivanja malware, virusa ili koda koji može uticati na boot proces servera), sistem za onemogućavanje nenamjernih izmjena nakon inicijalne konfiguracije), TPM 2.0 Administracija: lokalna i daljinska, uključuje napredne funkcije kao što su: directory services (AD, LDAP), dvofaktorska autentifikacija, single singn-on, PK autentifikacija, virtuelni folderi, daljinski file share, VNC veza sa operativnim sistemom, vitruelna konzola, kontrola snage (postavljanje granica i upozorenja), daljinsko instaliranje operativnog sistema Komplet šina za jednostavno postavljanje u rek i cable management Garancija: proizvođačka garancija minimum 3 godine	2.00	kom

		Platforma za virtualizaciju: VMware vSphere Essentials Plus Kit 3 hosts (max 2 CPU/host,max 32 cores/CPU socket) [VMware Software - [DSVQUIK]] (210-AIKY) Components 1 487-15781 3 Years ProSupport VMware vSphere 8 Essentials Plus Kit for 3 Hosts Sftwr Spt-Maint (ZR) Software 1 528-CUXR VMware vSphere 8 Ess Plus Kit for 3 hosts (Max 2 CPU per host, 32 cores/CPU),3YR Vmware SNS (ZR)		
2	Storidž sistem	Nabavka, isporuka i instalacija storidž sistema minimalno sledećih karakteristika: Storidž sistem mora da podržava minimum 24 x 2.5” hot-plug diska po enkložeru; podržava ukupno 272 diska uz dodatne enkložere potrebno je da podržava enkložere koji prihvataju do 84 x 3.5” diskova sa pojedinačnim kapacitetima do 20 TB storidž RAID controller, sa podrškom za: SSD, SAS i NLSAS diskove; RAID 1, 5, 6, 10, kao i distribuirani tip RAID koji kreira distribuirani rezervni (spare) prostor i na taj način omogućava aktivno korišćenje svih diskova sve vrijeme i ubrzava rebuild operacije tražena konfiguracija treba da ima minimum 8 x min 1.92TB SSD hot plug; Optimizacija: auto-tiering (do 3 primarna), Thin Provisioning , 1024 snapshota Mobilnost i migracija: asinhrona replikacija (jedan-na-više ili više-na-jedan), kopiranje kompletnih volume-a storidž je potrebno da ima redundantne kontrolere sa po minimum 4 (32 Gb FC) porta koji će omogućiti redundantnu konekciju servera; minimalno 16 GB memorije po kontroleru 2 management porta minimum 4 FC modula 32 Gb short wave FC transivera kompatibilnih sa ponuđenim storidžom; Form factor - 2U; Napajanje minimalno 550 W, redundantno Uz ponuđenu opremu je potrebno isporučiti i softver za nadgledanje servera i storage koji može pratiti inventar uređaja, aktivno stanje i alarmne situacije	1.00	kom

		Garancija: proizvođačka garancija minimum 3 godine		
3	Uređaj za skladištenje rezervnih kopija podataka	Nabavka, isporuka i instalacija uređaja za skladištenje rezervnih kopija podataka minimalno sledećih karakteristika: Rack server maximalno 2U. Procesor: minimum 1 x CPU 2.2 GHz (turbo frekvencija 2.7 GHz), 6 jezgara, 12 niti, 9 MB cache Memorija: minimalno 8 GB DDR4, podržano 64 GB memorije, server mora imati 4 memorijska slota. Storage Controller broj slotova mimum 12 2.5 ili 3.5 Disk: minimalno 6 x 8 TB SATA Hot Plug. Mreža: minimum 4 x 1Gb Ethernet portova, USB:minimalno 2 PCIe: minimalno 2 PCIe slots x8 Napajanje: 2 x 500 W Hot Plug Power Supply Uključene šine za rack. Garancija: proizvođačka garancija minimum 2 godine	1.00	kom
4	Backup platforma	Bekap rješenje mora da zadovoljava sljedeće kriterijume: Mora da podržava mogućnost instalacije na Windows OS, Linux OS, NAS. Mogućnost inastalacije kao virtuelni apliance ili Amazon machine image za AWS Mogucnost VMware i Hyper-V backup Funkcionalnosti minimalno za VMware: • zaštita podataka za vCentar i ESXi • mogućnost kreiranja sigurnosnih kopija bez agenta • trenutni recovery VM-ova, datoteka i objekata aplikacija • kopiranje VMware VM sigurnosne kopije van primarne lokacije, na traku ili pohranu u cloud • Automatsko testiranje sigurnosne kopije kako bi se provjerilo da li se podaci mogu oporaviti • Automatska zaštita preko polisa kako bi se uštedjelo vrijeme Funkcionalnosti minimalno za Hyper-V: • mogućnost kreiranja sigurnosnih kopija bez	1.00	kom

		agenta • trenutni granularni recovery • trenutni oporavak datoteka i objekata aplikacija direktno iz kompresovanih rezervnih kopija sa očuvanim svim dozvolama • Automatsko testiranje sigurnosne kopije kako bi se provjerilo da li se podaci mogu oporaviti • Automatska zaštita pomoću polisa, skripti i APIa Licenca i tehnička podrška u trajanju od minimum tri godine (36 mjeseci).		
	5 Security platforma za zaštitu email saobraćaja - Nabavka, isporuka i instalacija email antispam rješenja	Barracuda Email Security Gateway ili ekvivalent Minimalne karakteristike: Email Security Gateway mora da ima mogućnost filtriranja dolaznih poruke emailova i zaštitu email serverae od neželjenih i lažnih eemail poruka koji obuhvataju sledeće: neželjeni emailovi, zlonamjernog softvera, krađe identiteta, otkrivanja informacija, curenja podataka. Email Security Gateway mora da ima mogućnost filtriranja odlaznih emailova od neželjenih emailova i nepoželjnog sadržaja kako bi zaštitio reputaciju IP adresa i domena emailova i izbjegao unose na javne crne liste/liste odbijanja/liste blokiranja. Email Security Gateway mora da ima mogućnost da prima dolazne emailove preko SMTP, IMAP i POP protokola. Email Security Gateway mora da ima mogućnost da prosljeđuje dolazne i odlazne emailove preko SMTP protokola. Email Security Gateway mora da ima mogućnost da se konfiguriše pomoću Web korisničkim interfejsom. Email Security Gateway mora da ima mogućnost da podržava više domena. Virtuelna mašina Email Security Gateway mora da ima mogućnost da ima licencu za najmanje 2 virtuelna CPU-a. Filtriranje dolaznih emailova Filtriranje neželjenih mailova (Spam filtering) mora da ima sledeće mogućnosti: Klasifikacija neželjenih emailova mora da bude automatska i da funkcioniše bez potrebe za konfiguracijom ili finim podešavanjem. Klasifikacija neželjenih emailova mora da se zasniva na analizi namjere. Klasifikacija neželjenih emailova mora da se zasniva na	1.00	kom

traženju baze podataka o poznatim neželjenim prijetnjama (eng. Known-spam fingerprint database lookup). Klasifikacija neželjenih emailova mora da se zasniva na analizi slike sa optičkim prepoznavanjem znakova. Klasifikacija neželjenih emailova mora da podržava Bayesian mehanizam analize. Emailovi moraju da imaju mogućnost podešavanja spam ocjene (eng. Spam score). Administrator mora da ima mogućnost da mapira nivoe vjerovatnoće neželjenih mailova i sprovede odgovarajuće akcije; u zavisnosti od konfigurisanog nivoa vjerovatnoće, poruke treba da se obrađuju u četiri nivoa: prihvaćeni emailovi, označeni emailovi, emailovi u karantinu, blokirani emailovi. Tekst za označavanje emailova mora da ima mogucnost da se konfiguriše. Zaštita od zlonamjernog softvera (malware) mora da ima sledeće mogućnosti: Svi dolazni emailovi i prilozi moraju da se skeniraju sa najmanje tri nezavisna antivirusna mehanizma. Filtriranje zasnovano na reputaciji (Reputation-based filtering) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima bazu podataka reputacije IP adresa sa opcijom za blokiranje, karantin, označavanje ili onemogućavanje. Email Security Gateway mora da ima klasifikaciju emailova masovnog slanja da bi se prepoznali emailovi sa mailing liste, emailovi društvenih medija, marketinški emailovi sa opcijama za blokiranje, karantin, označavanje ili onemogućavanje. Email Security Gateway mora da ima integraciju sa Blok listama eksterne reputacije (External RBL). Filtriranje zasnovano na kontroli brzine (Rate control filtering) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost definisanja maksimalanog broja dolaznih konekcija po IP adresi u vremenskom period. Filtriranje pošiljaoca za dolazni email saobraćaj (Filtering of senders for inbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost stavljanja adrese emaila ili domena emaila na bijelu listu. Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja email adrese ili domena određenog pošiljaoca. Email Security Gateway mora da ima

mogućnost blokiranja, stavljanja u karantin ili označavanja emailova u slučaju neuspjele verifikacije SPF-a (Sender's Policy Framework). Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja emailova u slučaju neuspjele DKIM verifikacije (Domain Keys Identified Mail). Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja emailova koji dolaze sa IP adresa bez DNS PTR zapisa (reverse DNS verification). Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja emailova koji dolaze sa DNS domena specifičnih za državu ili domena najvišeg nivoa (npr. *.cn za Kinu). Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja emailova skupovima karaktera specifičnim za odabrane jezike.
Filtriranje primalaca za dolazne emailove (Filtering of recipients for inbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost stavljanja adrese emaila ili domena primaoca na bijelu listu. Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili označavanja email adrese ili domena određenog primaoca.
Filtriranje priloga za dolazne emailove (Filtering of attachments for inbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost blokiranja ili stavljanja u karantin emailova prema imenu priloga ili obrascu imena. Email Security Gateway mora da ima mogućnost blokiranja ili stavljanja u karantin emailova prema tipu MIME priloga. Email Security Gateway mora da ima mogućnost blokiranja ili stavljanja u karantin emailova prema kategoriji priloga; najmanje sledeće kategorije mora prepoznati: MS-Office dokumenti, PDF dokumenti, izvršne datoteke, multimedijalne datoteke, Windows skripte. Email Security Gateway mora da ima mogućnost blokiranja ili stavljanja u karantin emailova sa prilozima koji sadrže određene ključne riječi ili tekstualne obrasce.

Filtriranje sadržaja mailova (Message content filtering) mora da ima sledeće mogućnosti: Email Security Gateway mora

				da ima mogućnost blokiranja, stavljanja u karantin, označavamnja (eng. Tag) emailova sa određenim ključnim riječima ili obrascima u predmetu, zaglavlju ili tijelu email poruke. Odlazno filtriranje Filtriranje neželjene email pošte za odlazni saobraćaj (Spam filtering for outbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost klasifikacije neželjene email pošte koja treba da bude automatska i da funkcioniše bez potrebe za konfiguracijom ili finim podešavanjem. Email Security Gateway mora da ima mogućnost klasifikacije neželjene email pošte koja treba da se zasniva na analizi namjere. Email Security Gateway mora da ima mogućnost klasifikacije neželjene email pošte koja treba da se zasniva na analizi slike sa optičkim prepoznavanjem znakova. Email Security Gateway mora da ima mogućnost da emailovima dodijeljuje vjerovatnoću neželjene email pošte (spam score). Email Security Gateway mora da ima mogućnost da administrator može da mapira nivoe vjerovatnoće neželjene email pošte i u zavisnosti od konfigurisanih nivoa vjerovatnoće, emailovi moraju da budu obrađeni kao: prihvaćeni emailovi, emailovi u karantinu, blokirani emailovi. Zaštita od zlonamjernog softvera za odlazni email saobraćaj (Malware protection for outbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost da sve odlazne email poruke i priloge skenirati sa tri nezavisna antivirusna mehanizma. Filtriranje kontrole brzine odlaznog email saobraćaja za zaštitu reputacije i izbjegavanje crne liste (Rate control filtering of outbound traffic for reputation protection and blacklisting avoidance) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost da nametne/defineše maksimalan broj primalaca po pošiljaocu za određeni vremenski period. Filtriranje primalaca za odlazni email saobraćaj (Filtering of recipients for outbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost preusmjeravanja isporuke na email adrese ili domene na alternativni email server.		

Filtriranje priloga za odlazni email saobraćaj (Filtering of attachments for outbound traffic) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili preusmjeravanja email poruke sa prilozima određenog imena ili šablona imena. Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili preusmjeravanja email poruke prema tipu MIME priloga. Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili preusmjeravanja email poruke prema kategoriji priloga; najmanje sledeće kategorije treba prepoznati: MS-Office dokumenti, PDF dokumenti, izvršne datoteke, multimedijske datoteke, Windows skripte. Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili preusmjeravanja email poruke sa prilozima koji sadrže određene ključne riječi ili tekstualne obrasce.
Filtriranje sadržaja email poruka (Message content filtering) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost blokiranja, stavljanja u karantin ili preusmjeravanja email poruke sa određenim ključnim riječima ili obrascima u predmetu, zaglavlju ili tijelu email poruke.
Karantin i baferovanje poruka (Quarantine and message buffering) mora da ima sledeće mogućnosti: Email Security Gateway mora da ima mogućnost omogućavanja karantina po korisniku. Email Security Gateway mora da ima mogućnost omogućavanja email adrese u globalnom karantinu. Email Security Gateway mora da ima mogućnost baferovanja svih dolaznih i odlaznih email poruka i poništavanja odluka o blokiranju za pojedinačne email poruke (čak i blokirane email poruke treba da se mogu vratiti i isporučiti radnjom administratora).
Monitoring Email Security Gateway mora da ima ugrađeni monitoring dostupan putem web korisničkog interfejsa i da sadrži najmanje sledece karakteristike: monitoring storidža: iskorišten/slobodan prostor, performanse obrade i slobodni kapacitet, statistika poruka po satu, mogućnost SYSLOG integracija.
Izvještavanje Email Security Gateway mora da ima sistem izvještavanja koji je dostupan

putem web interfejsa i da sadrži najmanje sledece karakteristike: Planirani i trenutni izvještaji moraju biti dostupni za određene vremenske periode, sveobuhvatan skup izveštaja sa najmanje sledećim karakteristikama: pošiljaoce neželjene pošte, primaoce neželjene pošte, aktivnost virusa, veličine poruka, kršenja SPF-a. Email Security Gateway mora da ima upravljanje korisnicima i da sadrži najmanje sledece karakteristike: LDAP/Active Directory integracija za verifikaciju primaoca emailova, Podrška za LDAP, Radius ili lokalnu bazu podataka za verifikaciju pristupa korisnika za karantin po korisniku i korisničke postavke. Email Security Gateway mora da ima skalabilnost i visoku dostupnost sledećih karakteristika: podrška za grupisanje i federalni pristup baferu poruka (klasterirani uređaji su vidljivi kao jedan izvor podataka kada se poruke sortiraju i/ili oslobađaju od blokiranja), aktivno sa eksternim load-balancer. Email Security Gateway mora da ima mogucnost dnevnika poruka koji podrzumjeva sledeće: podrška za evidentiranje svih dolaznih i odlaznih poruka direktno sa sistema email gateway-a. Licenca u trajanju od minimum dvije godine (24 mjeseca).
Minimalne karakteristike: Rješenje mora biti kompatibilno sa Check point security gateway-ima.
Centralni management sistem mora da se isporuči u .iso formatu zajedno sa licencom koja omogućava upravljanje nad najmanje 5 firewall uređaja. Model licenciranja mora biti takav da ne sadrži ograničenja po pitanju korištenih resursa (CPU, Memorija, HDD). Rješenje mora imati mogućnost instalacije na najmanje sljedeće platforme Hyper-V (Windows 2016 Server и Windows 2012 Server R2), KVM (REHL 7 / CentOS 7), VMware vSphere 6.5/6.7) kao i Open server platforme.
Rješenje mora da ima mogućnosti: - Centralizovanog kreiranja bezbjednosnih pravila (eng. security policy) i distribuciju pravila na uređaje -Prikupljanje i čuvanje logova o saobraćaju kroz uređaj,
- Prikupljanje i čuvanje administratorskih logova (eng. audit logs)
- Korelaciju bezbjednosnih logova i prikazivanje izvještaja o statistici saobraćaja

		koji prolazi kroz uređaj za zaštitu informaciono komunikacione mreže (eng. Event Correlation) - Rješenje mora da posjeduje mogućnost korelacije bezbjednosnih događaja (eng. Event Correlation). - Rješenje mora da ima mogućnost grafičkog prikaza bezbjednosnih incidenata u mreži kroz predefinisane profile. - Rješenje mora da posjeduje mogućnost kreiranja izvještaja o bezbjednosnim incidentima kao i statistici saobraćaja. - -Rješenje mora da posjeduje predefinisane tipove izvještaja kao i mogućnost kreiranja novih tipova izvještaja shodno zahtjevu i potrebi korisnika. Rješenje mora da ima mogućnost kreiranja više administratorskih profila, sa različitim privilegijama pri čemu administrator mogu istovremeno da rade na istim bezbjednosnim pravilima bez međusobnog prekidanja rada (promjenu pravila i instalaciju pravila). Rješenje mora da ima integrisani x.509 CA (eng. certificate authority). Garancija i tehnička podrška: Dostupnost tehničke podrške proizvođača po principu 24x7 , Pristup bazi znanja (tehničkoj dokumentaciji) proizvođača, " Pristup bazi znanja (tehničkoj dokumentaciji) proizvođača, Uključena garancija i tehnička podrška u trajanju od minimalno 2 godine (24 mjeseca). U ponudi mora da bude uključen servis ažuriranja svih vrsta prijetnji u trajanju od 2 godine (24 mjeseca)."		
	6	Nabavka, isporuka i instalacija Security Management platforme:	Minimalne karakteristike: Rješenje mora biti kompatibilno sa Check point security gateway-ima. Centralni management sistem mora da se isporuči u .iso formatu zajedno sa licencom koja omogućava upravljanje nad najmanje 5 firewall uređaja. Model licenciranja mora biti takav da ne sadrži ograničenja po pitanju korištenih resursa (CPU, Memorija, HDD). Rješenje mora imati mogućnost instalacije na najmanje sljedeće platforme Hyper-V (Windows 2016 Server и Windows 2012 Server R2), KVM (REHL 7 / CentOS 7), VMware vSphere 6.5/6.7) kao i Open server platforme.	1.00	kom

		Rješenje mora da ima mogućnosti: - Centralizovanog kreiranja bezbjednosnih pravila (eng. security policy) i distribuciju pravila na uređaje -Prikupljanje i čuvanje logova o saobraćaju kroz uređaj, - Prikupljanje i čuvanje administratorskih logova (eng. audit logs) - Korelaciju bezbjednosnih logova i prikazivanje izvještaja o statistici saobraćaja koji prolazi kroz uređaj za zaštitu informaciono komunikacione mreže (eng. Event Correlation) - Rješenje mora da posjeduje mogućnost korelacije bezbjednosnih događaja (eng. Event Correlation). - Rješenje mora da ima mogućnost grafičkog prikaza bezbjednosnih incidenata u mreži kroz predefinisane profile. - Rješenje mora da posjeduje mogućnost kreiranja izvještaja o bezbjednosnim incidentima kao i statistici saobraćaja. - -Rješenje mora da posjeduje predefinisane tipove izvještaja kao i mogućnost kreiranja novih tipova izvještaja shodno zahtjevu i potrebi korisnika. Rješenje mora da ima mogućnost kreiranja više administratorskih profila, sa različitim privilegijama pri čemu administrator mogu istovremeno da rade na istim bezbjednosnim pravilima bez međusobnog prekidanja rada (promjenu pravila i instalaciju pravila). Rješenje mora da ima integrisani x.509 CA (eng. certificate authority). Garancija i tehnička podrška: Dostupnost tehničke podrške proizvođača po principu 24x7 , Pristup bazi znanja (tehničkoj dokumentaciji) proizvođača, " Pristup bazi znanja (tehničkoj dokumentaciji) proizvođača, Uključena garancija i tehnička podrška u trajanju od minimalno 2 godine (24 mjeseca). U ponudi mora da bude uključen servis ažuriranja svih vrsta prijetnji u trajanju od 2 godine (24 mjeseca)."		
7	Nabavka, isporuka i instalacija Security Gateway Sisitema:	Minimalne katakteristike: Rješenje mora biti kompatibilno sa Check point security gateway-ima.Traženo rješenje mora imati mogućnost implementacije u okviru softwerski definisanog datacentra zasnovanog na VmWare ESXI rješenju sa	2.00	kom

ciljem inspekcije saobraćaja Model licenciranja je zasnovan na broju virtuelnih korova dodijeljenih virtuelnoj mašini koja ga pokreće Tražena licenca 2 procesorska kora Perfomanse: Perfomanse ekvivalentne konfiguraciji 2 x vCore Intel xeon E5-2630 v3 / 8 GB RAM Memory Minimalni firewall throughput 7 Gbps NGFW propusna moć (firewall, application control i IPS) od najmanje 2,7 Gbps Propusna moć (firewall, application control, URL filtering, IPS, Antivirus AntiBoot) od najmanje 0,9 Gbps Firewall + IPS propusna moć od najmanje 3,9 Gbps Rješenje mora podržavati mogućnost rada u Active/Active L2, Active/Passive L2 i L3(routing) režimu rada Rješenje mora imati mogućnost kreiranja dinamičkih pravila (polisa) na osnovu identiteta dobijenih od najmanje sledećih izvora: Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers i 3rd parties uređaja kroz Web API integraciju.Rješenje mora da podržava mogućnost rada u MTA modu OSPFv2 and v3, BGP, RIP i Policy-based routing. Rješenje mora da uključuje sledeće bezbednosne servise: Application Control, URL filtering, Content Awareness, IPS, Anti-virus, Anti-Bot, Anti-Spam & Email zaštitu, zero-day zaštitu zasnovanu na cloud based i/ili on-premises SandBox tehnologiji, VPN, Remote Access VPN Rješenje mora da podržava DLP zaštitu kroz instalaciju dodatne licence bez kupovine dodatne opreme Rješenje mora imati mogućnost zero-day zaštite bazirane na cloud based i/ili on-premises SandBox tehnologiji za pretnje koje dolaze putem: HTTP, HTTPS, FTP, SMTP i SMTP TLS saobraćaja. Rješenje mora imati mogućnost emuliranja izvršnih fajlova, arhiviranih fajlova, dokumenata, JAVA i Flash aplikacija tj. Najmanje sledećih tipova dokumenata: 7z, cab, csv, doc, ocm, docx, dot, dotm, dotx, exe, jar, pdf, potx, pps, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, scr, swf, tar, tgz, xla, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip, gz, bz2. Rješenje mora imati mogućnost inspekcije SSL kriptovanog saobraćaja u dolaznom i odlaznom smeru Rješenje mora da ima mogućnost prepoznavanja najmanje 8000 internet aplikacija. Rješenje mora da ima mogućnost da koristi URL filtering pravila sa ciljem da omogući administratoru granularnu kontrolu

https inspekcije (bypass https inspection),Rješenje mora da ima najmanje 160 predefinisanih URL kategorija. Kroz Content Awareness bezbednosnu zaštitu. Rješenje mora da ima mogućnost prepoznavanja i kontrole najmanje sledečih tipova sadržaja koji se šalje odnosno preuzima kroz http & https: * Arhive, * CSV fajlovi, * database fajlova, * document fajlovi, * Executable fajlova, * Media i slike, * Presentation fajlova, * PCI Credit Card brojevi, Anti-Bot zaštita mora da ima mehanizam detekcije i blokiranja pristupa URL stranicama na osnovu reputacije URLa , Anti-Bot zaštita mora da ima mehanizam detekcije i blokiranja pristupa malicioznim domenima na osnovu reputacije domena, Anti-Bot zaštita mora da ima mehanizam detekcije i blokiranja sumnjivog (malicioznog) ponašanja u mreži Anti-Virus zaštita mora da ima mehanizam detektovanja malicioznih aktivnosti, Anti-Virus zaštita mora da ima mogućnost skeniranja arhiviranih fajlova , Anti-Virus zaštita mora da ima mogućnost blokiranja pristupa malicioznim URL stranicama, Anti-Virus zaštita mora da ima mogućnost skeniranja linkova unutar Email-a .Minimalne funkcionalnosti rješenja koje moraju biti podržane na menadžment softweru u sklopu licenci: Rješenje mora imati mogućnost kreiranja zaštitnih pravila (eng. security policy), prikupljanja, čuvanje i pregleda logova sa svih zaštitnih funkcionalnosti: firewall, IPS, URL filtering, application controll, Anti Virus i Anti Bot, zero-day zaštita. Konzola za upravljanje mora da ima grafički mehanizam za prikazivanje koliko je puta bezbjednosno pravilo bilo korišćeno (security rule hit counter). Za potrebe kreiranja bezbjednosnih pravila koristi se klijentska aplikacija koja se instalira na računarima administratora i koja omogućava menadžment svih bezbjednosnih pravila i koja se isporučuje u .exe formatu i koja se može instalirati neograničeno puta. Rješenje mora imati mehanizam verifikacije sigurnosnih polisa prije instalacije polisa (eng. security policy verification mechanism), Rješenje mora da imati mogućnost kreiranja revizije sigurnosnih polisa i mogućnost vraćanja na tu reviziju (eng. policy revision control mehanizam), Rješenje mora imati

		mogućnost jednostavnog i brzog kreiranja bezbjednosnih pravila korišćenjem mehanizma prevlačenja objekata (eng. drag & drop) u zaštitno pravilo, Rješenje mora imati mogućnost grupisanja bezbjednosnih pravila u slojeve (eng. layers) i kreiranja pod pravila unutar sloja (eng. sub layers), Rješenje mora imati mogućnost kreiranja više administratorskih korisnika, pri čemu administratori mogu istovremeno da rade na istom bezbednosnom pravilu bez međusobnog prekidanja rada (promenu pravila i instalaciju pravila), Rješenje mora imati mogućnost kreiranja više administratorskih profila, sa različitim privilegijama pri čemu administratori mogu istovremeno da rade na istom bezbjednosnom pravilu bez međusobnog prekidanja rada (promenu pravila i instalaciju pravila). Rješenje mora da ima mogućnost kreiranja administratorskih korisnika zavisno od njihove uloge. Npr. administratori koji imaju samo mogućnost praćenja: logova, URL pravila, IPS pravila. Rešenje mora imati integrisan interni x.509 CA (eng. certificate authority) softwerski zahtjevi i performanse security menadžment uređaja. Garancija i tehnička podrška: Dostupnost tehničke podrške proizvođača po principu 24x7 , Pristup bazi znanja (tehničkoj dokumentaciji) proizvođača, Uključena garancija i tehnička podrška u trajanju od minimalno 2 godine (24 mjeseca). U ponudi mora da bude uključen servis ažuriranja svih vrsta prijetnji u trajanju od 2 godine (24 mjeseca).		
8	Sistem za zaštitu Web saobraćaja (WAF)	Web aplikativni firewall na period od 3 godine (36 mjeseci) FortiWeb-VM (1 CPU) FC1-10-WBVMS-582-02-36 ili ekvivalent Ponuđeno rješenje mora da obezbjedi minimalno sledeće tehničke zahteve: Podrška za višenivovsku zaštitu Web aplikacija i API-ja od napada koji s koriste otkrivene i neotkrivene propuste na Webu, Uređaj mora da koristi napredne tehnike mašinskog učenja (na bazi veštačke inteligencije – AI) kako bi modelovao ponašanje svake aplikacije i uočio zlonamerne anomalije i blokirao ih, Uređaj mora da koristi tehnike zaštite kao što su: signature napada, IP adrese reputacija, provera protokola, IP adrese geo-lokacija, cross-site scripting, SQL injection i session	1.00	kom

hijacking, Uređaj mora da ima mogućnost povezivanja u jedinstvenu sigurnosnu arhitekturu sa firewall uređajima i sandbox sistemima, kako bi se omogućila razmjena sigurnosnih informacija i dublje skeniranje sumljivih fajlova, Podrška za zaštitu od OWASP Top 10 aplikacionih napada (Open Web Application Security Project 10 najkritičnijih rizika), Podrška za zaštitu API-ja (Application Programming Interface) i to: usklađenost XML i JSON protokola, API gateway i Web signature, Podrška za funkcionalnosti bot oslabljivanja i to: detekcija na bazi graničnih vrjednosti, detekciju biometrijskih bot-ova i poznatih bot-ova, Podrška za sledeće modove implementacije: reverse proxy, inline transparent i offline sniffing, Podrška za WCCP ili ekvivalentan protokol, Podrška za zaštitne mehanizme: SQL injection, Man-in-the-Browser, malware detekcija, validacija protokola, white listing, black listing, brute force zaštita, cookie signature i enkripcija, HTTP Header sigurnost, DOS sprečavanje, zaštita od poznatih i zero-day napada, zaštita od „curenja“ podataka (DLP), Mogućnost za rutiranje na osnovu sadržaja, HTTPS/SSL offloading, HTTP kompresiju, Layer 7 server load balancing, URL rewriting i keširanje, Podrška za upravljanje kroz grafički Web komandni intefejs, SNMP, Syslog, email logging, REST API i administrativne domene sa različitim ulogama administratora, Podrška za aktivnu i pasivnu autentifikaciju, Single Sign On (SSO), LDAP, RADIUS i SAML, SSL klijentske sertifikate i CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), Podrška za detaljnu grafičku analizu i izveštavanje u vidu ključnih elemenata: aktivnosti korisnika, IP konfiguracije, log zapisi napada i saobraćaja, mape napada i OWASP Top 10 kategorizaciju napada, Grafička analiza i izveštavanje mora da obezbede administratorima mreže informacije u realnom vremenu koje se odnose na izvor pretnje, koji je rizik za klijente i uređaje i uobičajene prekršaje, kako bi brzo identifikovali sumnjivu aktivnost, Podrška za opšte funkcionalnosti: IPv6, PKI integracija, čarobnjak (wizard) za podešavanje uobičajenih aplikacija i baza podataka,

		WebSocket i automatsko konfigurisanje kako bi se pojednostavila implementacija, Podrška za antivirusnom zaštitom koja skenira sve upload-ovane fajlove koji mogu inficirati servere ili druge elemente u mreži, Podrška za Web sigurnosni servis koji sadrži sumnjive URL šablone, signature na aplikativnom nivou, maliciozne robote, skener za update-e na Web ranjivosti (vulnerabilities) i modele prijetnji bazirane na mašinskom učenju, Podrška za servis IP reputacije koji štiti od poznatih izvora napada kao što su spammer-i, anonimni proxy-i i botnet-ovi, Mogućnost za servis zaštite kredencijala koji proverava da li se pokušaj pristupa (logovanja) nalazi na listi kompromitovanih kredencijala i preduzimanje akcija počevši od alarma do blokiranja pristupa za kredencijale (korisničko ime i lozinka) za koje se sumnja da su ukradeni, Propusnost za HTTP saobraćaj: minimalno 25 Mb/s, Propusnost za HTTPS saobraćaj: minimalno 10 Mb/s, Podrška za minimalno 4 administrativna domena, Podrška za povezivanje više uređaja u konfiguraciju visoke dostupnosti, Uključena podrška za neograničeni broj aplikacija ili uključene licence koje to omogućavaju (ukoliko sistem koristi licenciranje za aplikacije), Podrška za instalaciju na sledećem hardverskom sistemu: minimalno 1 vCPU i 8 GB memorije. Podrška za instalaciju na hipevizor i cloud sistemima: VMware, Microsoft Hyper-V, KVM, Citrix XenServer, Microsoft Azure, Google Cloud, Oracle Cloud, i Amazon Web Services, Uključena licenca za minimalno 3 godine koja omogućava minimalno sledeće funkcionalnosti: Web sigurnosni servis, servis IP reputacije, zaštita od malware-a, sandbox cloud servis, servis zaštite kredencijala i analitika pretnji. Mora biti uključena u cijenu trogodišnja tehnička podrška proizvođača po modelu 24x7.		
9	Sistem za centralizovano prikupljanje logova, analizu i reporting	Rješenje mora biti kompatibilno sa Fortigate uređajima. • Podrška za prikupljanje logova, analitiku i izveštavanje za firewall uređaj Fortinet FortiGate tako da kompatibilnost mora biti potvrđena u dokumentaciji proizvođača firewall uređaja, • Podrška za korelaciju događaja i detekciju	1.00	kom

u realnom vremenu za sve prikupljene logove,
• Podrška za dublju vidljivost i kritične mrežne vidljivosti kroz integraciju sa firewall uređajem FortiGate i sa sistemom za zaštitu Web saobraćaja
• Podrška za reagovanje u realnom vremenu na napade na mrežu, ranjivosti i upozorenje na potencijalna ugrožavanja, sa inteligencijom za pretnje, korelacijom događaja, nadgledanje, alarme i izvještavanje za trenutni taktički odgovor i oporavak,
• Podrška za automatizaciju kako bi odgovorilo na kritične alarme, događaje i SLA parametre (Service Level Agreement) za potrebe usaglašenosti sa regulativnom (compliance),
• Podrška za minimum 60 šablona izveštaja (report-a) i minimum 2.000 kombinovanih setova podataka, grafičkih dijagrama i makroa,
• Podrška za minimum sledeće formate report-a: CSV, PDF, HTML, JSON i XML,
• Podrška za servis indikatora kompromitovanosti sa minimalno 400.000 indikatora dnevno, koji u kombinaciji sa analitikom omogućavaju identifikovanje sumnjivih aktivnosti u mreži ili operativnom sistemu,
• Podrška za servis automatizacije sigurnosti koji se oslanja na skriptove, konektore i REST API kako bi se ubrzao odgovor na sigurnosne izazove i smanjilo vreme detekcije,
• Podrška za servis detekcije proboja sigurnosti (outbreak) koji sadrži pakete sadržaja kreiranih u realnom vremenu, kako bi se zaštitila mreža na nove malware proboje oktivene od strane globalne inteligencije za prijetnje. Paketi sadržaja mora da sadrže izvještaje, šablone izvještaja i akcije na događaje,
• Podrška za minimum 5 GB logova dnevno – centralno logovanje i analitika,
• Podrška za instalaciju na sledećem hardverskom sistemu: minimalno 4 vCPU i 8 GB memorije.
• Podrška za instalaciju na sa hipevizor i cloud sistemima: VMware, Microsoft Hyper-V, KVM, Citrix XenServer, Microsoft Azure, Google Cloud, Oracle Cloud, i Amazon Web Services

			• Uključena licenca za minimalno 3 godine koja omogućava minimalno sledeće funkcionalnosti: servis indikatora kompromitovanosti, servis automatizacije sigurnosti i servis detekcije proboja sigurnosti (outbreak), • Mora biti uključena u cijenu trogodišnja tehnička podrška proizvođača po modelu 24x7.		
	10	Uredjaj za neprekidno napajanje	Minimalne karakteristike: Tehnologija: Online double conversion Ulazni Priključak: socket IEC60320 C20 Ulazni Napon: 210-240 V Izlazni Priključci: 8 x IEC60320 C13, max. 10A per socket; 1 x IEC60320 C19, max. 16A per socket Snaga: 3000 VA Efikasnist: online 93 % ECO mode efikasnost: 98 %. Izmjenjive baterije u toku rada Kapacitet baterije: 6 x 12V x 9.0 Ah Punjenje baterije: Maximalno 4 časa do 90% kapaciteta nakon potpunog pražnjenja Mogućnost opcionog network menadžmenta Potrovi: USB, RS-232 Maksimalna temperatura rada: 0 - 40 °C Relativna vlažnost: 20 - 90% Maksimalne Dimenzije:19" 2RU Maksimalna težina:28 kg Bezbjedonosni standardi sertifikati: IEC/EN62040-1,IEC/EN60950-1 Elektromagnetni standardni sertifikati: IEC/EN62040-2,IEC61000-4-2,IEC61000-4-3,IEC61000-4-4, IEC61000-4-5,IEC61000-4-6,IEC61000-4-8 CE declaration Rek 19" UPS montažni kit (šine za rek ormar) Garancija: proizvođačka garancija minimum 2 godine	2.00	kom
	11	Usluga instalacije i konfiguracije	Usluge instalacije i konfigurisanja serverske i storadže opreme, kao i instalacija i konfiguracija ponuđenih rješenja i puštanje u operativan i funkcionalan rad. Integracija sa postojecom infrastrukturom u skladu sa zahtjevima i potrebama naručioca.	1.00	kom