HRVATSKE AUTOCESTE d.o.o. za upravljanje, građenje i održavanje autocesta, Širolina 4, 10 000 Zagreb

---

Evidencijski broj: I 5/17

POZIV ZA DOSTAVU PONUDE ZA:

NADOGRADNJA SUSTAVA ZA SIGURNOSNU ZAŠTITU TREND MICRO

Zagreb, listopad 2017. godine

1. NARUČITELJ

HRVATSKE AUTOCESTE d.o.o., Širolina 4, Zagreb, OIB: 57500462912

Internetska adresa: www.hac.hr

2. KONTAKT

Ime i prezime:	Lidija Svetec Šošić
Adresa elektroničke pošte:	lidija.svetec.sosic@hac.hr
Telefon:	+ 385 1 4694-774
Fax:	+ 385 1 4694-473

3. EVIDENCIJSKI BROJ NABAVE:

I 5/17

4. PROCIJENJENA VRIJEDNOST NABAVE:

150.000,00 kn (bez PDV)

5. PREDMET NABAVE

NADOGRADNJA SUSTAVA ZA SIGURNOSNU ZAŠTITU TREND MICRO

6. MJESTO IZVRŠENJA UGOVORA

Hrvatske autoceste d.o.o., Širolina 4, Zagreb

7. ROK IZVRŠENJA UGOVORA

Rok isporuke licenci, implementacije i integracije nadogradnje u postojeći sustav za sigurnosnu zaštitu Trend Micro je 30 (trideset) dana od dana stupanja Ugovora na snagu.

Rok pružanja usluge tehničke podrške sustava za sigurnosnu zaštitu Trend Micro je 12 (dvanaest) mjeseci od izvršene integracije nadogradnje.

8. KOLIČINA

Količina predmeta nabave određena je u Prilogu 4 -Troškovnik.

9. UGOVOR/NARUDŽBENICA

Naručitelj će s odabranim ponuditeljem sklopiti Ugovor pod uvjetima određenim u Prilogu 2 - Ugovor.

10. TRAŽENI DOKUMENTI

Dokumenti traženi ovom točkom mogu se dostaviti u obliku neovjerene preslike. Naručitelj može zatražiti dostavu izvornika te zadržava pravo provjere istih.

Ponuditelj mora dostaviti sljedeće dokumente:

10.1. Potvrda Porezne uprave o stanju duga ne starija od 30 dana računajući od dana slanja Poziva za dostavu ponude, kojom ponuditelj mora dokazati da je ispunio obvezu plaćanja dospjelih poreznih obveza i obveza za mirovinsko i zdravstveno osiguranje.

10.2. Potvrda ovlaštenog predstavnika proizvođača Trend Micro kojom ponuditelj dokazuje da ima partnerski status te da je ovlašten nuditi i prodavati Trend Micro proizvode kao i pružati uslugu održavanja i nadogradnji Trend Micro proizvoda.

10.3. Popis stručnih osoba koje će biti uključene u izvršenje ugovora, a koje posjeduju strukovnu sposobnost, stručno znanje i iskustvo potrebno za izvršenje ugovora.

Minimalan broj tehničkih stručnjaka koji se zahtijeva za izvršenje predmeta nabave:

- 1 (jedna) stručna osoba s certifikatom Trend Micro Certified Professional for Office Scan
- 1 (jedna) stručna osoba s certifikatom Trend Micro Certified Professional for Deep Discovery
- 1 (jedna) stručna osoba s certifikatom Trend Micro User Protection

Za navedene osobe potrebno je **priložiti certifikate o osposobljenosti** izdane od predstavnika proizvođača Trend Micro.

Certifikati mogu biti na hrvatskom i/ili engleskom jeziku.

11. CIJENA PONUDE

Ponuditelj je dužan ispuniti sve stavke u Troškovniku.

Ponuditelj dostavlja ponudu s cijenom izraženom u kunama, bez poreza na dodanu vrijednost (u daljnjem tekstu: PDV). Cijena ponude piše se brojkama.

Cijena ponude izražava se za cjelokupan predmet nabave i to na bazi Troškovnika iz ponude koju je dostavio Ponuditelj.

U cijenu ponude su uračunati svi troškovi i popusti, bez PDV. Ponuđene jedinične cijene iz Troškovnika su nepromjenjive i obuhvaćaju sve troškove i izdatke ponuditelja vezano za predmet nabave (osim PDV).

12. ROK, NAČIN I UVJETI PLAĆANJA

Rok način i uvjeti plaćanja propisani su u Prilogu 2 - Ugovor koji je sastavni dio ovog Poziva za dostavu ponude.

13. SADRŽAJ PONUDE

1. Ponudbeni list
2. Potvrda Porezne uprave
3. Potvrda ovlaštenog predstavnika proizvođača sukladno točki 10.2. Poziva za dostavu ponude
4. Popis stručnih osoba s certifikatima o osposobljenosti
5. Troškovnik (mora biti u potpunosti ispunjen i potpisan od ovlaštene osobe ponuditelja)

14. DOSTAVA PONUDE

Krajnji rok za dostavu ponude je: **27. listopada 2017. godine do 15,00 sati**

Ponuda se dostavlja na adresu: **HRVATSKE AUTOCESTE d.o.o.**

Zagreb, Širolina 4

Ponuda se dostavlja u zatvorenoj omotnici s naznakom:

''PONUDA ZA - EV.BROJ: I 5/17 – NADOGRADNJA SUSTAVA ZA SIGURNOSNU ZAŠTITU TREND MICRO - NE OTVARAJ''

15. OTVARANJE PONUDA

Otvaranje ponuda neće biti javno.

16. KRITERIJ ODABIRA NAJPOVOLJNIJE PONUDE

Naručitelj će kao najpovoljniju ponudu izabrati ponudu s najnižom cijenom, koja u potpunosti udovoljava svim traženim uvjetima Naručitelja.

Prije donošenja odluke Naručitelj može pozvati ponuditelja na pregovaranje i/ili izmjenu i/ili nadopunu ponude sukladno svojim zahtjevima i potrebama.

17. ODLUKA O ODABIRU/PONIŠTENJU

Odluka o odabiru/poništenju dostavlja se ponuditeljima elektroničkom poštom te se objavljuje na web-stranici Naručitelja.

18. PRILOZI

- Prilog 1: Ponudbeni list
- Prilog 2: Ugovor
- Prilog 3: Tehnički opis
- Prilog 4: Troškovnik

PRILOG 1 - PONUDBENI LIST

NARUČITELJ: Hrvatske autoceste d.o.o., Širolina 4, 10000 Zagreb,
OIB: 57500462912

PONUDBENI LIST

Broj ponude: _____

Datum ponude: _____

Ponuditelj: _____

Adresa: _____

OIB: _____

IBAN: _____

Kontakt osoba: _____

Adresa e-pošte: _____

Broj telefona: _____

Broj faksa: _____

Dostavljamo Vam ponudu za:

NADOGRADNJA SUSTAVA ZA SIGURNOSNU ZAŠTITU TREND MICRO, EV.BROJ: I 5/17

Izjavljujemo da smo u cijelosti proučili i prihvatili uvjete ovog Poziva i Tehničkog opisa te Vam sukladno istom dostavljamo ponudu za cijenu

Cijena ponude bez PDV: _____

Rok valjanosti ponude je **60 (šezdeset) dana** od dana isteka roka za dostavu ponuda, te je moguće prihvatiti ovu ponudu u bilo kojem roku, do isteka konačnog roka.

ZA PONUDITELJA: _____
(Potpis)

OVLAŠTEN ZA POTPIS PONUDE: _____
(Ime, prezime i funkcija)

PRILOG 2 - UGOVOR

HRVATSKE AUTOCESTE d.o.o. za upravljanje, građenje i održavanje autocesta, Zagreb, Širolina 4, OIB: 57500462912 (u daljnjem tekstu: Naručitelj), koje zastupa .....

i

.....OIB:..... (u daljnjem tekstu: Isporučitelj), koje zastupa .....

sklopili su sljedeći

UGOVOR

PREDMET

Članak 1.

Predmet Ugovora je **NADOGRADNJA SUSTAVA ZA SIGURNOSNU ZAŠTITU Trend Micro** (u daljnjem tekstu: Roba), a u svemu prema pozivu za dostavu ponude Naručitelja od ..... 2017. godine, ponudi Isporučitelja broj: …… od……2017. godine, Tehničkom opisu i Troškovniku koji se nalaze u privitku ovog Ugovora i čine njegov sastavni dio.

CIJENA

Članak 2.

Cijena za izvršenje Ugovora iznosi:

UKUPNO: kn

(slovima:)

Cijena iz stavka 1. ovog članka iskazana je bez poreza na dodanu vrijednost (u daljnjem tekstu: PDV). PDV mora biti posebno iskazan, a obračunavat će se prema važećim zakonskim propisima.

Jedinične cijene iz Troškovnika su nepromjenjive i obuhvaćaju sve troškove i izdatke Isporučitelja vezano za izvršenje Ugovora, osim PDV.

Jedinične cijene su na paritetu fco lokacija Naručitelja iz članka 3. ovog Ugovora.

Količine određene u Troškovniku su točne.

MJESTO IZVRŠENJA UGOVORA

Članak 3.

Mjesto izvršenja Ugovora je u poslovnoj zgradi Naručitelja na adresi: Širolina 4, Zagreb.

ROK IZVRŠENJA UGOVORA

Članak 4.

Isporučitelj se obvezuje izvršiti isporuku licenci, implementaciju i integraciju nadogradnje u postojeći sustav za sigurnosnu zaštitu Trend Micro u roku od 30 (trideset) dana od dana stupanja ovog Ugovora na snagu.

Isporučitelj se obvezuje pružati uslugu tehničke podrške sustava za sigurnosnu zaštitu Trend Micro 12 (dvanaest) mjeseci od izvršene integracije nadogradnje.

OBVEZE UGOVORNIH STRANA

Članak 5.

Isporučitelj se obvezuje:

- isporučiti licence, izvršiti implementaciju i integraciju nadogradnje u postojeći sustav za sigurnosnu zaštitu Trend Micro sukladno svim zahtjevima iz Tehničkog opisa i Troškovniku,
- po izvršenoj integraciji nadogradnje u postojeći sustav za sigurnosnu zaštitu Trend Micro izraditi Zapisnik o primopredaji te dostaviti odgovornoj osobi Naručitelja na ovjeru,
- tehničku podršku sustava za sigurnosnu zaštitu Trend Micro pružati sukladno svim pravilima struke i zahtjevima iz Tehničkog opisa.

Članak 6.

Naručitelj se obvezuje:

- omogućiti Isporučitelju nesmetan pristup do mjesta izvršenja Ugovora.

PREGLED IZVRŠENE ISPORUKE, IMPLEMENTACIJE I INTEGRACIJE

Članak 7.

Prije početka isporuke Robe, Isporučitelj će obavijestiti odgovornu osobu Naručitelja iz članka 13. ovog Ugovora (u daljem tekstu: Odgovorna osoba Naručitelja) te će zajednički utvrditi točan termin isporuke.

Odgovorna osoba Naručitelja dužna je odmah po izvršenju integracije nadogradnje u postojeći sustav za sigurnosnu zaštitu Trend Micro na uobičajeni način izvršiti pregled te ispitati funkcionalnost istog, u nazočnosti odgovorne osobe Isporučitelja.

Odgovorna osoba Naručitelja će nakon izvršenog pregleda i utvrđivanja ispravnosti rada sustava za sigurnosnu zaštitu Trend Micro sukladno svim uvjetima iz članka 5. ovog Ugovora, ovjeriti Zapisnik o primopredaji.

Odgovorna osoba Naručitelja neće ovjeriti Zapisnik o primopredaji u ukoliko sustav za sigurnosnu zaštitu Trend Micro nije u skladu sa svim uvjetima iz članka 5. ovog Ugovora te

će o eventualnim nedostacima obavijestiti Isporučitelja bez odgađanja. Isporučitelj se obvezuje iste ukloniti u primjerenom roku određenom od strane odgovorne osobe Naručitelja, računajući od dana primitka pisane obavijesti Naručitelja. U slučaju da se obavijest predaje na ruke Isporučitelju, isti primitak obavijesti potvrđuje potpisom.

Članak 8.

O skrivenim nedostacima, koji nisu bili uočljivi u času pregleda, odgovorna osoba Naručitelja je dužna obavijestiti Isporučitelja bez odlaganja.

Takve nedostatke Isporučitelj je dužan ukloniti u primjerenom roku od dana primitka pisane obavijesti Naručitelja. Isporučitelj snosi punu odgovornost za sve skrivene nedostatke isporučene Robe.

PLAĆANJE

Članak 9.

Isporučitelj će isporučenu Robu obračunati prema stvarno izvršenim količinama i jediničnim cijenama iz Troškovnika.

Isporučitelj će ispostaviti račun s danom isporuke Robe i bez odgađanja ga, zajedno sa primjerkom Zapisnika o primopredaji, dostaviti odgovornoj osobi Naručitelja na ovjeru.

Odgovorna osoba Naručitelja dužna je račun ovjeriti u roku od 3 (tri) dana od dana zaprimanja. Ukoliko račun nije ispostavljen sukladno Ugovoru vraća se Isporučitelju na ispravak.

Ovjera računa neće se izvršiti ukoliko Naručitelju nije dostavljeno Jamstvo sukladno članku 10. ovog Ugovora.

Naručitelj se obvezuje ovjereni račun platiti u roku od 30 (trideset) dana od dana zaprimanja.

Ako Naručitelj ne plati Isporučitelju u roku navedenom u prethodnom stavku ovog članka, Isporučitelj ima pravo na zateznu kamatu sukladno zakonskim odredbama.

Prenošenja tražbine po Ugovoru ne mogu se ugovarati bez pisanog pristanka Naručitelja.

JAMSTVO

Članak 10.

Isporučitelj se obvezuje u roku 8 (osam) dana od dana zaprimanja obostrano potpisanih primjeraka ovog Ugovora dostaviti Naručitelju Jamstvo za uredno ispunjenje ugovora te za osiguranje potraživanja Naručitelja u slučaju raskida ugovora u iznosu koji pokriva 10% (deset posto) Cijene iz članka 2. ovog Ugovora. Jamstvo se podnosi u obliku bjanko zadužnice sukladno Pravilniku o obliku i sadržaju bjanko zadužnice (NN 115/12).

Naručitelj ima pravo naplate Jamstva 13 (trinaest) mjeseci od dana ovjere Zapisnika o primopredaji.

UGOVORNA KAZNA

Članak 11.

Ukoliko Isporučitelj svojom krivnjom ne izvrši ugovorne obveze u roku iz članka 4. ovog Ugovora, za svaki dan prekoračenja ugovornog roka Naručitelj će zaračunati Isporučitelju ugovornu kaznu u iznosu od 0,25% Cijene iz članka 2. ovog Ugovora, koja ugovorna kazna ne može prekoračiti 5% Cijene iz članka 2. ovog Ugovora.

Naručitelj ne može zahtijevati ugovornu kaznu zbog zakašnjenja, ako je primio zakašnjelo isporučenu Robu, a nije bez odgađanja priopćio Isporučitelju da zadržava svoje pravo na ugovornu kaznu.

Odgovorna osoba Naručitelja u ovom slučaju mora pisanim putem bez odgađanja obavijestiti Izvršitelja da zaprima zakašnjelo isporučenu Robu, ali zadržava pravo na ugovornu kaznu.

RASKID UGOVORA

Članak 12.

Za slučaj da Isporučitelj ne ispuni ugovorne obveze na način kako je ugovoreno, Naručitelj će pozvati Isporučitelja da obvezu ispuni u naknadnom primjerenom roku. Ukoliko Isporučitelj ni u naknadnom roku ne ispuni obvezu, Naručitelj je ovlašten raskinuti ugovor.

Troškovi koji bi nastali na strani Naručitelja temeljem takvog postupanja Isporučitelja, u cijelosti padaju na teret Isporučitelja.

Naručitelj u slučaju iz stavka 1. ovog članka ima pravo i na naknadu štete.

ODGOVORNE OSOBE

Članak 13.

Odgovorne osobe za izvršenje ovog Ugovora su:

- Za Naručitelja: , telefon: , e-mail: ,
- Za Izvršitelja: , telefon: , e-mail: .

Odgovorne osobe iz stavka 1. ovog članka će međusobnu komunikaciju obavljati elektroničkim i/ili pisanim putem.

U slučaju promjene odgovorne osobe iz stavka 1. ovog članka, svaka ugovorna strana dužna je pisanim putem obavijestiti drugu ugovornu stranu o nastaloj promjeni.

Takva pisana obavijest smatrat će se izmjenom stavka 1. ovog članka i neće se posebno ugovarati, te će činiti sastavni dio ovog Ugovora.

ZAVRŠNE ODREDBE

Članak 14.

Ovaj Ugovor stupa na snagu danom potpisa one ugovorne strane koja ga potpiše kasnije.

Članak 15.

Sastavni dio ovog Ugovora čine:

- Poziv za dostavu ponude Ev.broj: I 5/17
- Tehnički opis
- Troškovnik
- Ponuda Isporučitelja broj: ..... od ..... 2017. godine
- Jamstvo za uredno ispunjenje ugovora.

Članak 16.

Ugovorne strane suglasne su da će eventualne sporove iz ovog Ugovora rješavati dogovorno, a u protivnom ugovaraju nadležnost suda u Zagrebu.

Članak 17.

Ovaj Ugovor sastavljen je u 6 (šest) istovjetnih primjerka, od toga 2 (dva) primjerka za Isporučitelja i 4 (četiri) primjerka za Naručitelja.

ZA ISPORUČITELJA: ZA NARUČITELJA:

Urbroj: 4211-160- /2017

Ev.broj: I 5/17

U Zagrebu,

PRILOG 3 – TEHNIČKI OPIS

TEHNIČKI OPIS

ZA NADMETANJE EV. BROJ: I 5/17

NADOGRADNJA SUSTAVA ZA SIGURNOSNU ZAŠTITU TREND MICRO

Cilj integracije/nadogradnje Trend Micro proizvoda je proširenje postojećih funkcionalnosti kroz mogućnost korelacije detekcije kroz sve točke zaštite i detekcije.
Konkretno postojeće rješenje Naručitelja Deep Discovery Email Inspector posjeduje „sandboxing“ (odnosno izvršavanje potencijalnog malwarea i zaraženih dokumenata kako bi otkrio njihovo maliciozno ponašanje) koji generira jedinstveni „pattern“ koji postaje dio sigurnosnog rješenja u samoj organizaciji.
Ovaj način omogućuje uspješnu detekciju i obranu od tzv. „zero day“ napada:

- Ukoliko su napadi ciljani na pojedinu organizaciju, proizvođači sigurnosnih rješenja nisu mogli proizvesti „pattern“ obzirom da napad nije do sad viđen.
- Ukoliko napad i nije ciljan, ali je organizacija među prvim žrtvama napada, napad će biti uspješan jer postoji period kašnjenja s detekcijama napada iz gore navedenog razloga.

Trend Micro Officescan na računalima i poslužiteljima je nadogradnja „sandboxing“ tehnologije jer „pattern“ detektiranih napada u „sandboxu“ implementira na samo računalo (koji je najčešće i cilj nekakvog napada). Korištenjem Trend Micro Officescana datoteke detektirane u „sandboxu“ kao maliciozne biti će prepoznate i direktno na računalu neovisno na koji način ih napadač pokuša dostaviti na samo računalo (usb, privatni email koji ne prolazi korporativnu zaštitu, web…).

Kako bi navedena korelacija detekcije bila prožeta kroz cijelu IT infrastrukturu rješenje mora sadržavati zaštitu za sljedeću infrastrukturu:

- Zaštita radnih stanica i poslužitelja od virusa, spywarea i ostalih malicioznih programa
- Softversko rješenje koje omogućuje virtualne zakrpe za često korištene aplikacije i operacijske sustave u svrhu zaštite od poznatih i nepoznatih ranjivosti te sigurnosnih propusta
- Softversko rješenje za zaštitu mail prometa od virusa i spama te filtriranje sadržaja, integrirano sa Exchange sustavom
- Softversko rješenje u obliku virtualnog računala za zaštitu mail prometa od virusa i spama te filtriranje sadržaja na perimetru mreže
- Softversko rješenje u obliku virtualnog računala za zaštitu Internet (WEB) prometa od virusa i filtriranje sadržaja na perimetru mreže

Obzirom na korelaciju detekcije koja sadrži više proizvoda, svi proizvodi se moraju moći konfigurirati, nadgledati i održavati kroz jedinstveno web sučelje.
Također rješenje mora sadržavati mogućnost jedinstvene autentikacije korisnika za sigurnosne proizvode unutar organizacije.

U kratko, Trend Micro rješenja moraju omogućiti Naručitelju direktno konzumiranje znanja o nepoznatim napadima korištenjem Deep Discovery Email Inspectora na svim klijentima, poslužiteljima i točkama kroz koje prolazi mail i Internet (web) promet sa i prema korisniku.

Ponuditelj je nakon završene implementacije i integracije s postojećim rješenjem obavezan osigurati podršku u trajanju od 12 mjeseci. Potrebna količina licenci koja će se isporučiti

prilikom nadogradnje je 350 komada, tip: TrendMicro Enterprise Security Suite, 350 User License. Ponuditelj se obavezuje osigurati podršku za navedene licence u trajanju od 12 mjeseci.

Naručitelj koristi cca 270 Windows klijenata (desktop računala + prijenosna računala) i 75 poslužiteljskih računala koje je potrebno zaštititi traženim rješenjem.
Od navedenih 75 poslužitelja, 2 su Exchange CAS poslužitelja, 2 Exchange DAG poslužitelja, dok su ostali uglavnom aplikacijski poslužitelji i na njima je potreban file scanning antivirusni software.

Zaštita radnih stanica i servera od virusa, spywarea i ostalih malicioznih programa

Softversko rješenje za zaštitu od virusa, spyware-a i ostalog malicioznog koda na radnim stanicama i serverima uz centralno upravljanje i praćenje virusnih incidenata u mreži.

Karakteristike i funkcije:

- zaštita radnih stanica i servera od svih vrsta malicioznih programa (virusi, crvi, spyware, grayware i ostali srodni programi),
- klijentski firewall sa konfiguracijom parametara prema smjeru, vrsti prometa te aplikaciji, u potpunosti integriran u antivirusni klijent i konzolu za upravljanje, uz jednostavno udaljeno definiranje firewall politike;
- integrirana real-time zaštita od mrežnih crva i detekcija iskorištavanja propusta na IP nivou (napr. Downad/Conficker i srodne varijante mrežnih crva);
- integrirana detekcija poremećaja u mrežnom prometu (klijentski IPS/IDS sustav), uključujući tipične napade na IP nivou (Ping of death, SYN flood, Teardrop, itd.);
- automatsko centralizirano čišćenje zaraženih računala bez intervencije administratora; u potpunosti integrirano u antivirusni klijent (čišćenje registry zapisa, ini zapisa, memorijskih procesa koje ostavljaju crvi, itd.);
- automatsko čišćenje spyware programa u potpunosti integrirano u antivirusni klijent;
- zaštita od web baziranog zlonamjernog koda;
- blokiranje pristupa malicioznim web stranicama na razini klijenta temeljeno na reputaciji IP adrese ili URL-a; mogućnost definiranja fleksibilne politike filtriranja ovisno o lokaciji i statusu klijenta;
- provjera reputacije datoteka (file reputation) na klijentu putem direktnog kontaktiranja servera ili online servisa proizvođača;
- Automatsko prikupljanje informacija o prijetnjama i automatsko ažuriranje proizvođačeve reputacijske baze.
- POP3 Mail Scan provjera na viruse i spam integrirana u klijentu;
- nadgledanje ponašanja klijenta (Behavior monitoring) sa „In The Cloud“ provjerom da li je aplikacija poznata i sigurna;
    - mogućnost povratka datoteka koje su karantenirane kao sumnjive, centralno putem administratorske konzole te uz definiranje iznimaka od budućeg karanteniranja
- mogućnost definiranja fleksibilnih i granularnih politika (po klijentu ili grupama klijenata) nadzora ponašanja aplikacija, a što uključuje sumnjive radnje poput: izmjene hosts datoteke, kreiranja duplikata poznate sistemske datoteke, instalacije novog plugin-a za Internet Explorer, izmjene postavki u Internet Exploreru, izmjene Windows Security Policy-a, ubacivanja novog DLL-a za svaki pokrenuti proces,

kreiranja novog startup programa, itd. Za svaku od ovih sumnjivih radnji moguće je definirati različite akcije: od blokiranja, preko upozorenja i logiranja do dozvole rada.

- mogućnost definiranja fleksibilnih i granularnih politika (po klijentu ili grupama klijenata) kontrole pristupa vanjskim uređajima na klijentu (izmjenjivi mediji koji se spajaju preko USB-a);
- blokiranje Autorun funkcije kod spajanja USB diskova na klijent;
- kontrola pristupa mrežnim resursima i dijeljenim diskovima (network shares);
- provjera web prometa uz sandboxing tehnologiju koja sprječava pokretanje malicioznih web skripti i iskorištavanje sigurnosnih propusta u browseru, uz blokiranje prije isporuke na real-time scan.
- detekcija i logiranje C&C bot aktivnosti uz granularnu konfiguraciju akcije po otkrivanju mrežne komunikacije prema C&C poslužiteljima
- opcionalna podrška za VDI okruženja (virtualizacija desktopa): mogućnost ograničavanja potrošnje resursa virtualnih radnih stanica na razini hosta - VMware vCenter (VMware View), Citrix XenServer 5.5 (Citrix XenDesktop 4). Mogućnost pre-scana master VDI image-a te kontrolirani deployment komponenti za ažuriranje na pojedinom VDI hostu.
- podrška za podešavanje CPU potrošnje prilikom provjere file-ova (scanning);
- integrirana podrška za distribuciju update komponenti u scenarijima sa slabijim bandwidthom;
- podržano više izvora ažuriranja komponenti prema IP adresi;
- centralna administracija preko web konzole dostupne sa bilo kojeg računala u mreži, odnosno izvana uz korištenje edge reley komponente
- podrška za Active Directory: automatska provjera sukladnosti odnosno detekcija računala koja nemaju antivirusnu zaštitu, a na osnovu informacija iz AD-a;
- podrška za integraciju sa više različitih Active Directory izvora (kod pružanja upravljane usluge za više AD domena)
- kod pristupa web konzoli, podržana integracija sa MS Active Directory-em, odnosno autentifikacija preko account-ova iz AD-a (single signon) uz mogućnost definiranja prava pristupa (administrator, power-user, read-only user,...) za pojedine dijelove admin sučelja i/ili grupe klijenata
- više metoda daljinske instalacije na klijente: NT remote install, login skripte, MSI Active directory group policy deployment, SMS sever deployment, e-mail deployment, putem third-party rješenja za distribuciju softvera;
- web bazirana instalacija sa klijenta (preko web stranice konzole), tzv. web deployment;
- opcionalna podrška za zaštitu Macintosh računala;
- integracija sa korporacijskim jedinstvenim web upravljačkim sučeljem za sve antivirusne produkte na svim razinama kako bi se dobio jedinstveni pregled aktivnosti i centralno konfiguriranje više rješenja
- proaktivna zaštita od provale virusa i novih nepoznatih prijetnji uz mogućnost blokiranja vektora širenja crva i virusa, kao što je zabrana pisanja u shared foldere, blokiranje mrežnih portova i zapisa datoteka;
- verifikacija potpisa MSI paketa prije instalacije programa te mogućnost zabrane instalacije nepoznatih programa skinutih putem HTTP ili mail kanala;
- automatska integracija sa rješenjem za otkrivanje naprednih prijetnji putem sandboxinga: automatsko sprečavanje napada na endpointu, a na temelju sumnjivih informacija dobivenih kroz automatiziranu sandbox analizu (sumnjivi promet, izmjene sustava, itd.)

- ransomware zaštita: proaktivno blokiranje malicioznih programa koji preuzimaju kontrolu nad računalom i/ili kriptiraju dokumente na računalu
- mogućnost upravljanja svim klijentskim računalima, neovisno jesu li u lokalnoj mreži ili izvan nje, ukoliko je postavljena edge reley komponenta
- statička (analiza svojstava datoteke) i dinamička (analiza ponašanja datoteke) analiza korištenjem machine learning algoritmima

Virtualne zakrpe

Rješenje koje daje mogućnost postavljanja sigurnosne politike za zaštitu računala krajnjih korisnika na nivou mreže u vidu firewall te IDS/IPS funkcija. Pruža funkcije tzv. Host based Intrusion Prevention System (HIPS) rješenja, što uključuje tkz. virtualne zakrpe za često korištene aplikacije i operacijske sustave, u svrhu zaštite od poznatih i nepoznatih ranjivosti te sigurnosnim propustima.

- Dvosmjerni statefull inspection firewall
- Zaštita od ranjivosti (virtual patching)
- Mogućnost paralelne instalacije sa tradicionalnim anti-malware rješenjem (npr. Trend Micro OfficeScan)
- Centralizirano prikupljanje logova sa klijenta
- Centralizirano upravljanje klijentima
- Prilagodljivi dashboard (kontrolna ploča) koristeći tzv. widgete, uz mogućnost dubinske analize događaja (drill-in);
- Alati za nadzor, izvještaje i automaska upozorenja
- Mogućnost generiranja i eksportiranja izvještaja;
- Integrirano tkz. "virtualno patrhiranje" (eng. Virtual patching), automatska zaštita od poznatih sigurnosnih propusta u softveru (operacijskom sustavu, preglednicima, poznatim aplikacijama), bez potrebe za instalacijom službenih zakrpa proizvođača.
- IPS/DPI provjere (HIPS) u realnom vremenu ili na zahtjev (manual/scheduled)
- Dvosmjerni tzv. stateful inspection firewall za zaštitu računala/servera, uz definiranje kriterija prometa: IP adresa, MAC adresa, vrsta prometa (TCP, UDP, ICMP, itd), smjer prometa, aplikacija, sadržaj (sigurnosni propust);
- Zaštita od premošćivanja komunikacija između dva mrežna sučelja (primjenom ograničenja na upotrebu jednog mrežnog sučelja spriječava tuneliranje komunikacija sa npr. wireless sučelja preko wired VPN sučelja u enterprise.)
- Mogućnost postavljanja sigurnosnih politika na pojedina računala korištenjem predefiniranih ili vlastito izrađenih sigurnosnih profila (npr. profili za Windows XP, 7, 8 računala), a koji mogu uključivati bilo koju od gore navedenih sigurnosnih provjera (DPI, firewall);
- Automatsko ažuriranje definicija o sigurnosnim prospustima (virtual patching), uz mogućnost granularne automatske primjene;
- Definiranje politike ovisno o preporuci dobivenoj na temelju automatizirane provjere sustava (Recommendation scan)
- Detektiranje otvorenih portova na krajnjem računalu (Port Scan)
- Podržani operacijski sustavi:
    - Windows 8.1 (32-bit i 64-bit),
    - Windows Server 2012 R2 (64-bit),
    - Windows 8 (32-bit i 64-bit),
    - Windows Server 2012 (64-bit),
    - Windows 7 (32-bit i 64-bit),

- Windows Server 2008 R2 (64-bit),
- Windows Server 2008 (32-bit i 64-bit),
- Windows Vista (32-bit i 64-bit),
- Windows Server 2003 SP1 (32-bit i 64-bit) sa patchem "Windows Server 2003 Scalable Networking Pack",
- Windows Server 2003 SP2 (32-bit i 64-bit),
- Windows Server 2003 R2 SP2 (32-bit i 64-bit),
- Windows XP (32-bit i 64-bit)

Rješenje za zaštitu mail prometa od virusa i spama te filtriranje sadržaja, integrirano sa Exchange sustavom

Softversko rješenje za zaštitu mail prometa od virusa i spama te filtriranje sadržaja, integrirano sa Exchange sustavom

- podržan Exchange 2010, 2013, 2016;
- kompletna integracija sa Exchange 2010, 2013, 2016 rolama (Edge, Hub, Mailbox Server, Combo Server, Clustered Mailbox Server),
- integracija sa Exchange cluster okruženjem (Exchange Virtual Servers - EVS)
- podrška za VERITAS cluster okruženja
- podržava Exchange Database Availability Groups (DAG)
- integracija sa System Center Operations Manager
- Mogućnost instalacije na više Exchange servera istovremeno (udaljena instalacija)
- podrška za Microsoft VSAPI 2.5, 2.6
- SMTP način pretraživanja mail prometa
- definiranje iznimaka za priloge i filtriranje sadržaja uz upotrebu integracije sa Microsoft Active Directory-em
- podržan Single Sign-On sa Microsoft Active Directory kredencijalima
- definiranje administrativnih rola sa različitim pravima pristupa
- praćenje administrativnih aktivnosti putem log-a
- Podrška za IPv6
- SSL web konzola za upravljanje
- Real-time i ručno pretraživanje Exchange Information Store-a i mailboxova
- Integracija sa organizacijskim jedinstvenim web upravljačkim sučeljem za antimalware proizvode na svim razinama (endpoint, gateway, itd.)
- provjera prometa na viruse, malware i spyware u realnom vremenu
- ručna provjera ili u predefiniranim intervalima (scheduled scan) cijelog Information Store-a, uz mogućnost inkrementalne provjere (diferencijal u odnosu na prethodnu provjeru)
- korištenje naprednih heurističkih metoda detekcije kako bi se otkrila iskorištavanja propusta u dokumentima i privicima (attachments)
- mogućnost automatskog proslijeđivanja poruka/privitaka u kojima je utvrđeno sumnjivo ponašanje (npr. pokušaj iskorištavanja određenog propusta) na rješenje za tzv. sandboxing sumnjivih datoteka i URL-ova. Mogućnost konfiguriranja politike ovisno o rezultatu sandbox analize
- Izbjegavanje dvostruke provjere mail prometa ukoliko je ista već napravljena na Hub Transport roli
- proaktivna zaštita od provale virusa,
- granularna antispam provjera prometa
- pretraživa karantena uz mogućnost slanja/propuštanja karanteniranih poruka

- korisnička spam karantena uz integraciju sa Outlook Junk E-mail folderom
- upotreba Web reputacije za filtriranje poruka koje sadrže maliciozne URL-e (u tijelu poruke kao i attachmentu)
- provjera datoteka na malware dodatno koristi proizvođačev servis za provjeru datoteka u cloud-u
- filtriranje konekcija upotrebom IP reputacije - odbijaju se sve konekcije od poznatih izvora spama
- filtriranje sadržaja maila po svim djelovima poruke (tijelo poruke, sadržaj i tip attachmenta) i ključnim riječima
- Mogućnost pretrage mailboxova uz selektivno brisanje mailova (i drugih objekata poput sastanaka, itd.) koji sadrže nepoželjni sadržaj. Funkcija mora biti dostupna samo administratorima sa odgovarajućom rolom.
- ograničenje procesorskog opterećenja za provjeru prometa.
- Automatska nadogradnja definicija u predefeiniranim intervalima ili na zahtjev administratora
- slanje obavijesti i uzbuna u slučaju detekcija malwarea/spam-a i/ili nepoželjnog sadržaja
- Detaljni pregled logova i izvještaja (uz mogućnost slanja mailom)

Softversko rješenje u obliku virtualnog računala za zaštitu mail prometa od virusa i spama te filtriranje sadržaja na perimetru mreže

Rješenje za zaštitu od zlonamjernog koda i neželjene pošte (spama) na razini SMTP i POP3 prometa, na centralnoj točki pristupa internetu (Internet gateway).

Rješenje mora biti isporučeno u obliku Virtualnog Appliancea, uz podršku za *bare metal* instalaciju na hardver te instalaciju na virtualne platforme Vmware i Microsoft HyperV.

Minimalna podrška za virtualizaciju:

- VMware ESX/ESXi
- Microsoft Hyper-V

Osnovne funkcionalnosti zaštite od neželjene pošte

- Pretraživanje i provjera SMTP prometa
- Pretraživanje i provjera POP3 promet
- Provjera na malware i spyware u svim dijelovima poruke
- Proaktivna zaštita od provale virusa (outbreak prevencija)
- Zaštita od različitih varijanti e-mail crva putem heurističke detekcije kompresijskih algoritama
- Detekcija spama korelacijom poruka sa online servisom koji sadrži najnovije informacije o spam porukama
- Zaštita od neželjenih poruka (spama)
- Heuristička detekcija exploitova u dokumentima: zaštita od zero-day prijetnji, detekcija exploit koda u dokumentima, detekcija poznatih ranjivosti

- E-mail reputacija: potpuno integrirana zaštita od spama filtriranjem na IP nivou provjerom reputacije adrese poslužitelja pošiljatelja
- Dinamička analiza web linkova unutar poruka u smislu spam provjere. Upotreba web reputacijskog filtriranja za provjeru reputacije URL-a unutar email poruka
- Posebna detekcija poruka koje koriste socijalni inženjering za isporuku malwarea i krađu podataka
- Posebna klasifikacija tzv. graymail poruka

Dodatne funkcionalnosti filtriranja poruka

- Filtriranje sadržaja mail poruke prema različitim dijelovima poruke (sva header polja te tijelo poruke) kao i sadržaja privitaka (attachment)
- Mogućnost kreiranja vlastitih blacklista i whitelista po kriteriju pune mail adrese ili domene pošiljatelja i primatelja
- Automatska integracija sa rješenjem za otkrivanje naprednih prijetnji putem sandboxinga: mogućnost slanja attachmenta na sandbox analizu te blokiranje poruka ovisno o pronađenom sumnjivom ponašanju datoteke unutar sandboxa.
- Rewriting sumnjivih URL-ova u porukama za uvijek ažurnu zaštitu od malicioznih web odredišta

Dodante funkcionalnosti zaštite i upravljanja mail prometom

- Integrirano Cloud bazirano filtriranje - mogućnost odstranjivanja neželjne pošte u cloud servisu proizvođača, prije dolaska poruke i/ili konekcije do e-mail gatewayja
- Podrška za DKIM (Domain Key Identified Mail) u dolazu i potpisivanje u odlazu
- Podrška za Sender Policy Framework
- Provjera bounce mailova i sprječavanje bounce (*backscatter*) napada
- Automatska prevencija Directory Harvest Attack napada (DHA)
- Detekcija nepravilno formuliranih (malformed) poruka
- Zaštita od mail-baziranog DoS napada
- Podrška za TLS uz mogućnost selektivnih postavki kriptiranja na transportnom nivou ovisno o domeni primatelja poruke
- Mogućnost dodavanja korporativne poruke o odricanju od odgovornosti
- Upravljanje SMTP i HTTPS certifikatima kroz web sučelje proizvoda
- Detekcija lažiranih (eng. spooded) poruka
- Mogućnost odgode isporuke mail poruke za određeno doba dana

Ostale tehničke i sistemske funkcionalnosti

- Od strane proizvođača prema sigurnosnim preporukama konfiguriran operacijski sustav
- Integriran firewall
- Web sučelje za administraciju
- Centralizirano izvještavanje
- Mogućnost definiranja vlastitih izvještaja i prikaza unutar web sučelja za administraciju
- Mogućnost definiranja različitih rola za pristup administracijskom sučelju
- Mogućnost pregleda toka pojedinih poruka kroz web sučelje (message tracking)
- Mogućnost integracije sa centralnim upravljačkim sučeljem za sva sigurnosna rješenja proizvođača

- Integracija sa višestrukim LDAP imenicima kod definiranja politika
- Karantena kojom može upravljati krajnji korisnik uz autentikaciju preko LDAP-a odnosno Active Directoryja
- High-availability
    - Centralna web konzola za administraciju svih uređaja i praćenje logova
    - Sinkronizacija konfiguracije među svim uređajima u clusteru
- Integriran softver baze podataka za skladištenje logova
- Mogućnost exporta i importa konfiguracije
- Syslog integracija za agregaciju logova
- Kontrola količine poruka primljenih od određenog servera pošiljatelja (SMTP rate control)
- Audit log
- Podrška za korištenje eksterne baze podataka

Softversko rješenje u obliku virtualnog računala za zaštitu Internet (WEB) prometa od virusa i filtriranje sadržaja na perimetru mreže

Rješenje za zaštitu od zlonamjernog koda te kategorizacije sadržaja na razini HTTP, HTTPS i FTP prometa, na centralnoj točki pristupa internetu (Internet gateway).

Rješenje mora biti isporučeno u obliku Virtualnog Appliance-a, uz podršku za *bare metal* instalaciju na hardver, te instalaciju na virtualne platforme Vmware i Microsoft HyperV.

Minimalna podrška za virtualizaciju:

- VMware: ESX/ESXi
- Microsoft: Hyper-V

Karakteristike i funkcije:

- Podrška za više načina za integraciju u mrežnu infrastrukturu:
    - Cisco WCCP
    - Transparent Bridge način rada
    - Eksplicitni proxy (postavke definirane na klijentu ručno ili kroz PAC/WPAD skriptu)
    - Reverzni proxy
    - ICAP integracija

- Podrška za IPv6
- Provjera reputacije datoteka (file reputation) putem direktnog kontaktiranja servera ili online servisa proizvođača
- Mogućnost dobivanja visoke raspoloživosti servisa (High availability) kroz active/passive clustering
- Mogućnost replikacije konfiguracije na više instalacija
- Command Line Interface za nadzor u realnom vremenu, detekciju i otklanjanje problema, administraciju
- Web sučelje za administraciju
- Mogućnost definiranja različitih rola za pristup administracijskom sučelju
- Mogućnost integracije sa centralnim upravljačkim sučeljem za sva sigurnosna rješenja proizvođača

- Centralizirano izvještavanje
- Upravljanje Proxy Auto-config (PAC) datotekom bez dodatnog web servisa
- Mogućnost dinamičke URL kategorizacije u realnom vremenu za nekategorizirane URL-ove
- Integriran cache za Internet sadržaje
- Skeniranje HTTP prometa na viruse i druge sigurnosne prijetnje, uz granularno postavljanje politike za tipove datoteka i akcije nad njima.
- Mogućnost antimalware provjere na temelju tzv. cloud baze definicija u realnom vremenu
- Skaniranje FTP prometa uz blokiranje datoteka po definiranim tipovima i formiranja odvojene politike za komprimirane datoteke
- Detekcija stvarne „ekstenzije„ datoteke analizom početnog dijela datoteke
- Mogućnost suradnje sa drugim HTTP i FTP proxy serverima
- Napredno „odgođeno skeniranje" za velike datoteke za HTTP i FTP
- Definiranje politike i blokiranje Java appleta i ActiveX kontrola na osnovu provjere certifikata objekta u svrhu zaštite od malicioznog mobilnog koda
- Instrumentacija Java appleta radi: nadzora izvršavanja nedozvoljenih akcija, automatskog blokiranja izvršavanja na klijentu ili upozorenja i upita korisnika za dozvolu izvršenja
- Definiranje povjerljivih URL-a za koja se ne provodi skeniranje i blokiranje objekata skaniranja
- Privremeno blokiranje URL-a za koje je skeniranjem sadržaja u toku rada utvrđeno da sadrže maliciozne programe
- Prepoznavanje i kontrola web baziranih aplikacija (Application Control)
- Detektiranje i blokiranje zaraženih računala unutar kompanije naprednom analizom mrežnog prometa (Botnet Detection)
- Detekcija i blokiranje komunikacije prema komandnim i konktrolnim serverima (C&C Contact Callback Detection)
- Otkrivanje i blokiranje ciljanih napada (APT - Advance Persistent Threat) putem emulacije ponašanja preglednika (browser)
- Napredna analiza dokumenata za otkrivanje zlonamjernog koda te integracija sa sandboxing rješenjem proizvođača
- Integracija sa višestrukim LDAP imenicima kod definiranja politika
- Definiranje kvota pristupa za korisnike po dnevnim, tjednim i mjesečnim limitima
- Identifikacija klijenata po IP adresi, imenu računala i LDAP-u
- Ograničenje pristupa Internetu za klijente, i ograničenje pristupa pojedinim serverskim portovima
- Prilagodljive notifikacije administratorima (putem emaila) i korisnicima o sigurnosnim i drugim događajima.
- SNMP notifikacija za sigurnosne događaje, ažuriranje programa i paterna, kao i probleme rada servisa
- Podesivi pragovi i vrijednosti za sistemske notifikacije administratoru
- Primjena URL filtriranja i blokiranja zlonamjernih sadržaja dohvatom kategorije URL-a putem upita „on-line" servisu proizvođača, bez upotrebe lokalne kategorizacijske baze
- Anonimna povratna informacija proizvođaču o detektiranim inficiranim URL-ovima radi ažuriranja „on-line" servisa
- Filtriranje web opasnosti putem dohvata ocjene o reputaciji stranice/ip adrese kojoj korisnik pristupa – filtriranje po web reputaciji. Zaštita od web baziranog

zlonamjernog koda; blokiranje pristupa malicioznim web stranicama temeljeno na reputaciji IP adrese ili URL-a
- Filtriranje i blokiranje URL-a prema kategorijama i vremenskom rasporedu, kao i pojedinačno definiranih URL adresa
- Zaštita korisnika od phishing web stranica primjenom Web reputacije i liste phishing URL-a u pattern datoteci koja se redovno ažurira,
- Detekcija i blokiranje nepoželjnog „Instant messaging (IM)" i konekcija autentikacijskih protokola tuneliranih kroz port 80

Centralno web upravljačko sučelje za antivirusne proizvode na svim razinama

Jedinstveno web sučelje koje omogućuje instalaciju, konfiguraciju, motrenje i održavanje svih antivirusnih aplikacija na svim razinama mreže uz njihovu međusobnu koordinaciju.

Karakteristike i funkcije:

- centralno upravljanje zaštitom,
- daljinsko upravljanje,
- Web sučelje,
- integracija zaštite radnih stanica, servera, Exchange sustava, Internet gateway-a;
- integrirani servisi za prevenciju provale virusa;
- integrirani servisi za uklanjanje posljedica virusa, trojana, crva i spywarea;
- multi-tier struktura upravljanja, skalabilnost;
- Jedinstveno i izvješćivanje i logging, te kreiranje izvještaja u PDF, RTF i HTML formatima.
- podrška za Windows klijentske operativne sustave: XP, Vista; Windows 7, Windows 8 i 8.1, Windows 10
- podrška za serverske operativne sustave: Windows 2003, Windows 2008, Windows 2012, Windows 2016
- podrška za 32 i 64-bitne verzije operativnih sustava;
- podrška za 64-bitnu arhitekturu procesora;
- podrška za virtualizirana okruženja