Robert Trivunčević, NORT d.o.o.

Ekskluzivni distributer ESET NOD32 proizvoda na tržištu
Hrvatske, BiH, Srbije, Crne Gore, Kosova, Makedonije i Albanije

Koje su najčešće opasnosti za računala?

Virusi **Crvi**

Trojanci **Rootkit** **Backdoor**

Spyware **Botnet** **Keylogger** **Dialer**

Spam **Phishing** **Adware**

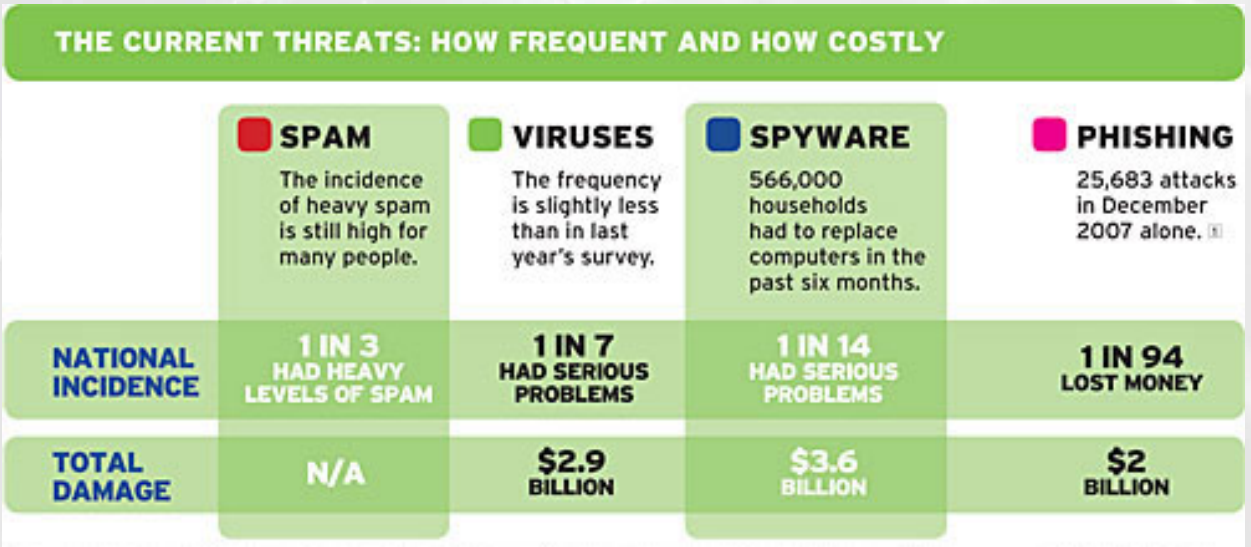
Svjesnost o prisutnosti opasnosti

- ***Nevidljivi*** **- potpuno prikriveni maliciozni rad bez vanjskih manifestacija, dugo vremena neotkriveni i tiho izvršavaju svoju zadaću**
- ***Vidljivi*** **- agresivni, ometaju rad, ucjenjuju zaraženog korisnika**

Kolika je šteta?

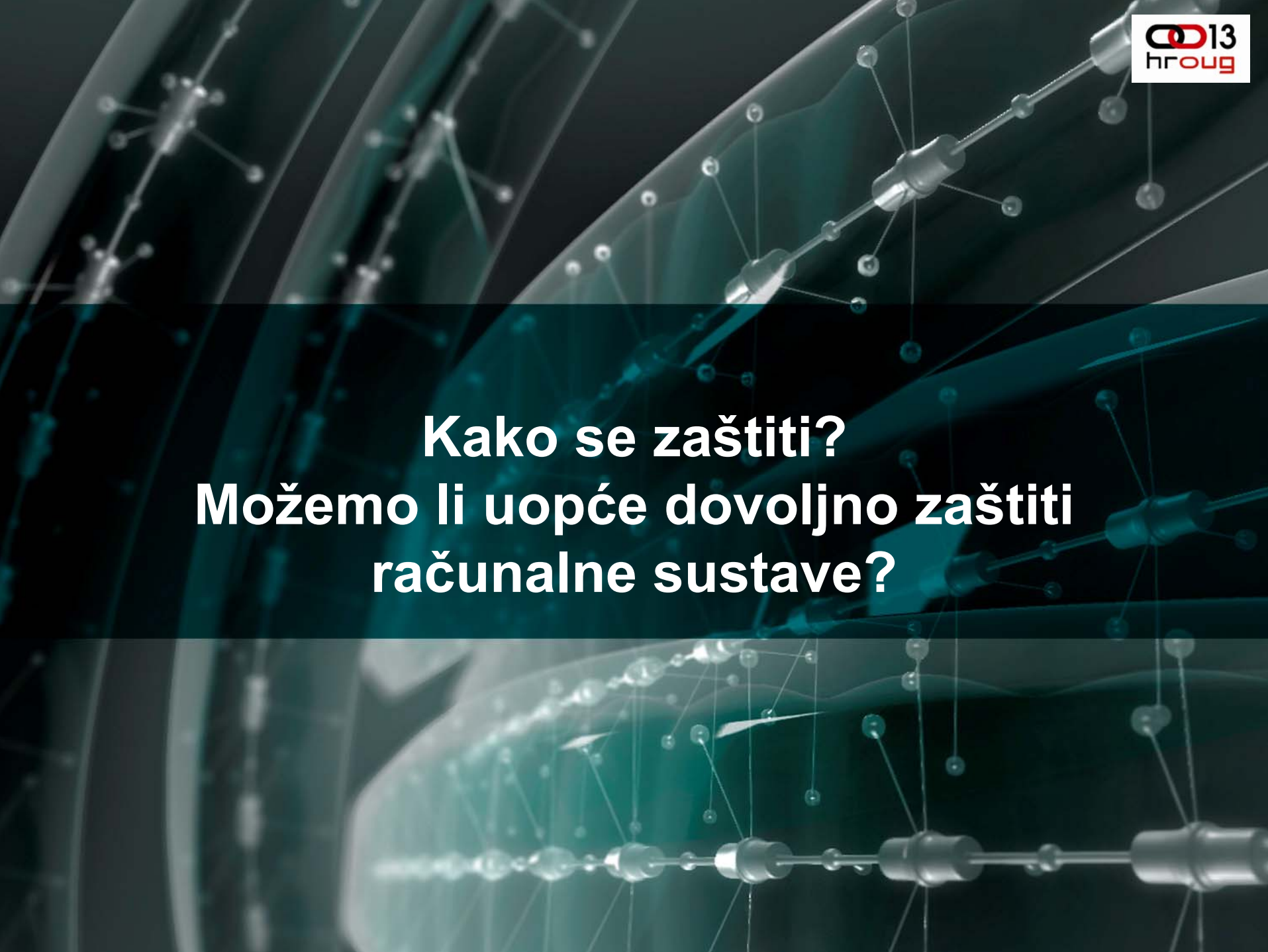
Expert • Independent • Nonprofit
ConsumerReports.org®

Izvještaj za rujan 2008.



THE CURRENT THREATS: HOW FREQUENT AND HOW COSTLY

	SPAM	VIRUSES	SPYWARE	PHISHING
	The incidence of heavy spam is still high for many people.	The frequency is slightly less than in last year's survey.	566,000 households had to replace computers in the past six months.	25,683 attacks in December 2007 alone.
NATIONAL INCIDENCE	1 IN 3 HAD HEAVY LEVELS OF SPAM	1 IN 7 HAD SERIOUS PROBLEMS	1 IN 14 HAD SERIOUS PROBLEMS	1 IN 94 LOST MONEY
TOTAL DAMAGE	N/A	$2.9 BILLION	$3.6 BILLION	$2 BILLION


Kako se zaštiti?
Možemo li uopće dovoljno zaštiti
računalne sustave?

Ovo je obična zaštitna kaciga

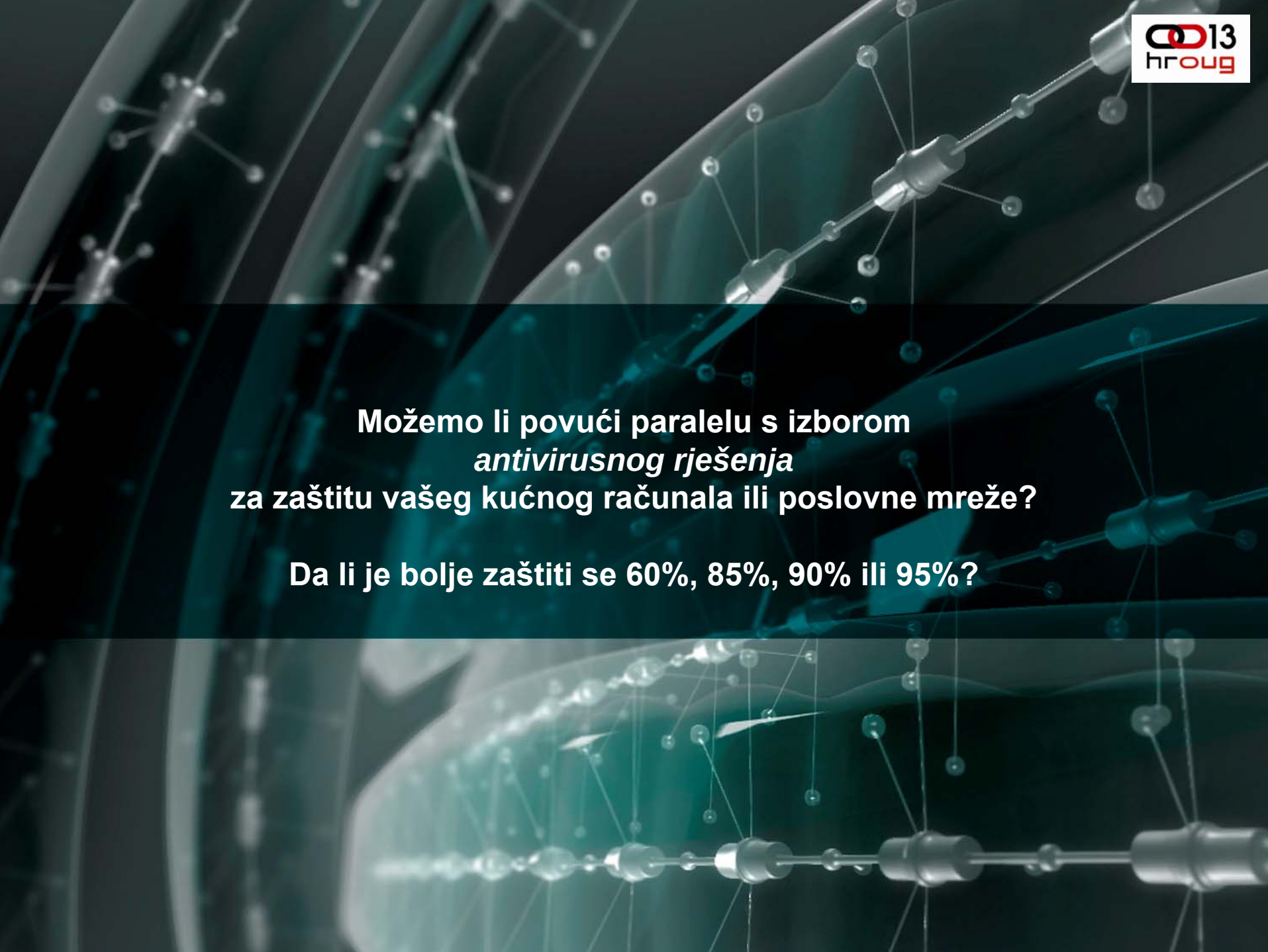
Amortizira 60% kinetičke energije udarca

Kaciga postrojbi za specijalne operacije

Amortizira 90% kinetičke energije udarca
Štiti i od udara metka, šrapnela i sl.

A ovo je baseball palica...

Koju od prethodno prikazanih kaciga biste željeli imati na glavi ako bi vas netko htio udariti ovom palicom? ☺☺

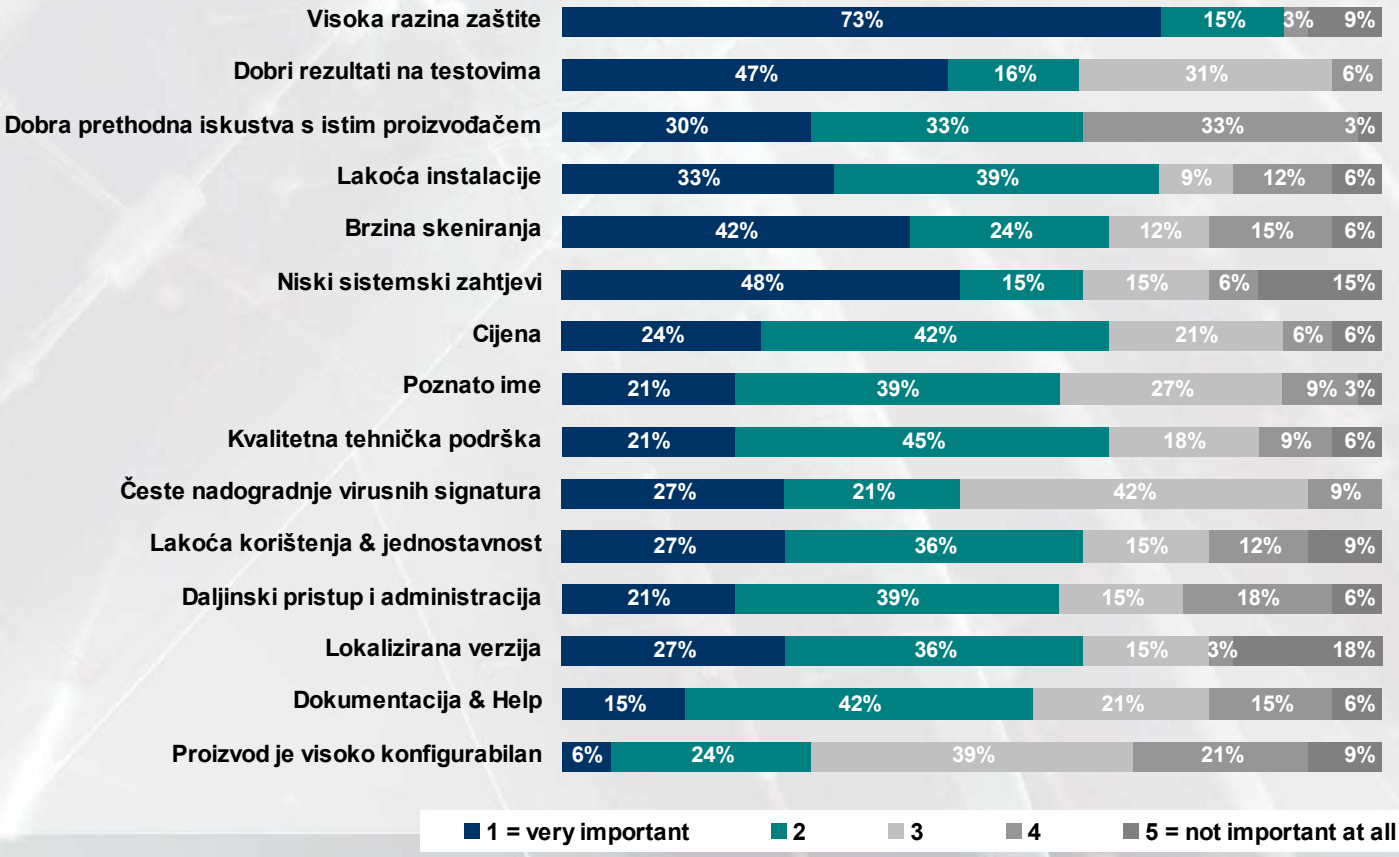


Možemo li povući paralelu s izborom
antivirusnog rješenja
za zaštitu vašeg kućnog računala ili poslovne mreže?

Da li je bolje zaštiti se 60%, 85%, 90% ili 95%?

Anketiranje korisnika, što očekuju od sigurnosnih programa?

Koji od dolje navedenih faktora su značajni za kupce pri izboru sigurnosnih programa?



Izvor: BBDO May 2007

Što korisnici žele?

1. Visoku razinu zaštite
   - Proaktivno
   - Zaštita od kombiniranih prijetnji
2. Niski sistemski zahtjevi
3. Preciznost
4. Veliku brzina skeniranja
5. Vrhunsku tehničku podršku
6. Lokaliziranu verziju

Ključne prednosti ESET-ovih rješenja

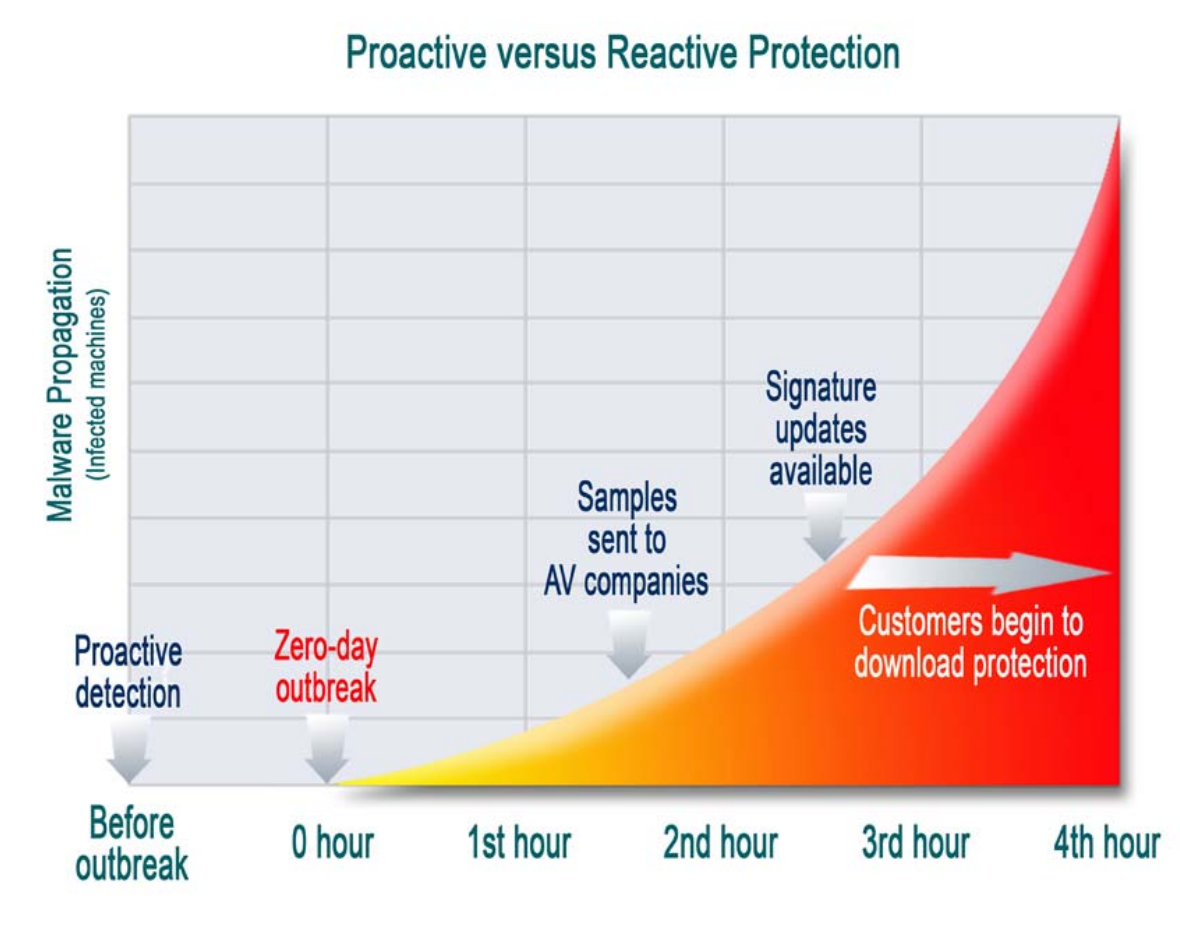
1. Vrhunska detekcija poznatih i još nepoznatih opasnosti
2. Mali utjecaj na sistemske resurse
3. Velika brzina skeniranja

Što mi podrazumjevamo heuristikom

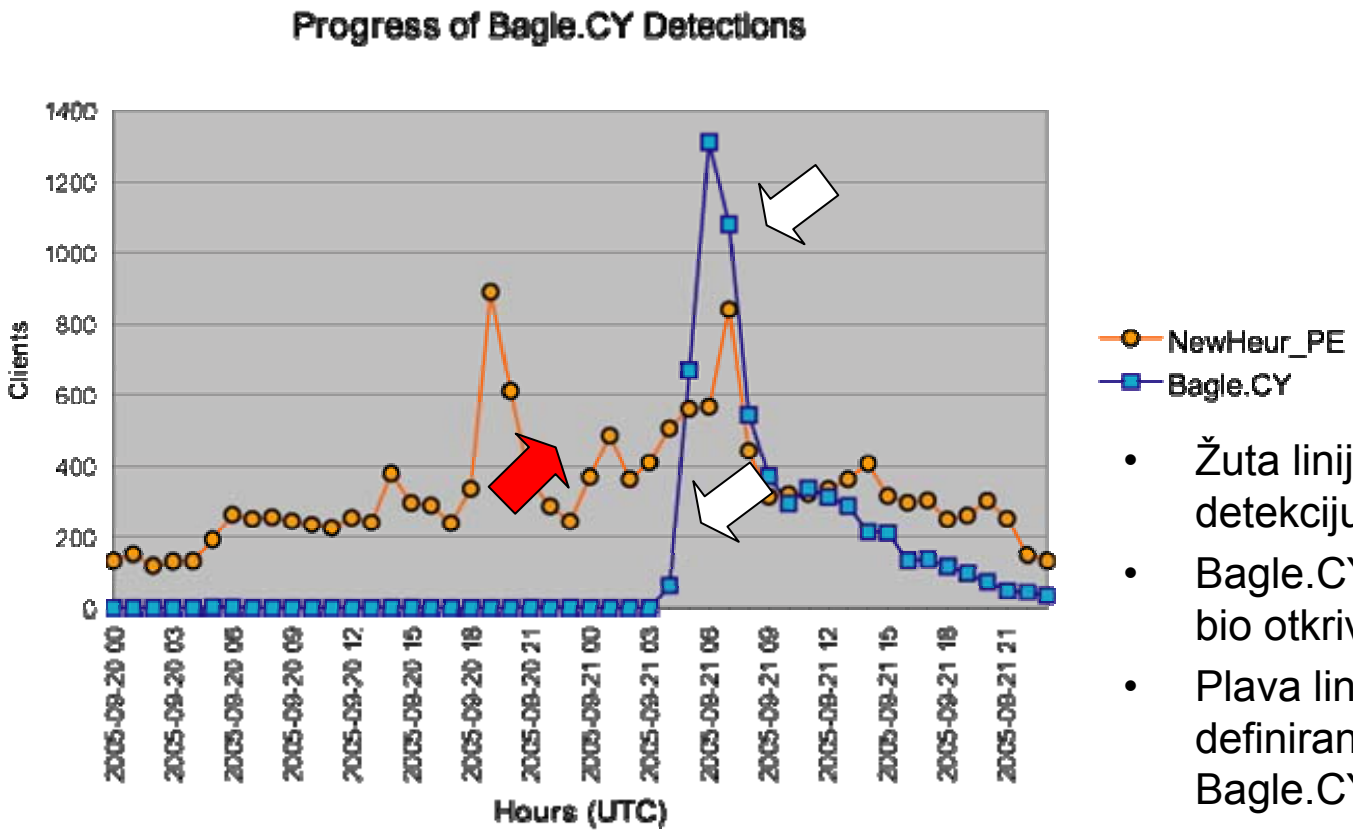
Heuristički sistem igra ulogu 'virtualnog istraživača virusa"

- Emulacija nam omogućuje sigurno okruženje u kojem se može ispitati delovanje malwarea, ukloniti enkripcija itd.
- Sve znanje koje posedujemo o delovanju malwarea jeste 'rečeno' analitičkom kodu
- Zlonamjeran kod je zatvoren i ne može djelovati na stvarnom sistemu računala
- Dobro balansiran 'rezultat' umanjuje mogućnost za 'false positives'
- Heuristika može biti često nadograđivana kako bismo osigurali da je uvijek optimalna

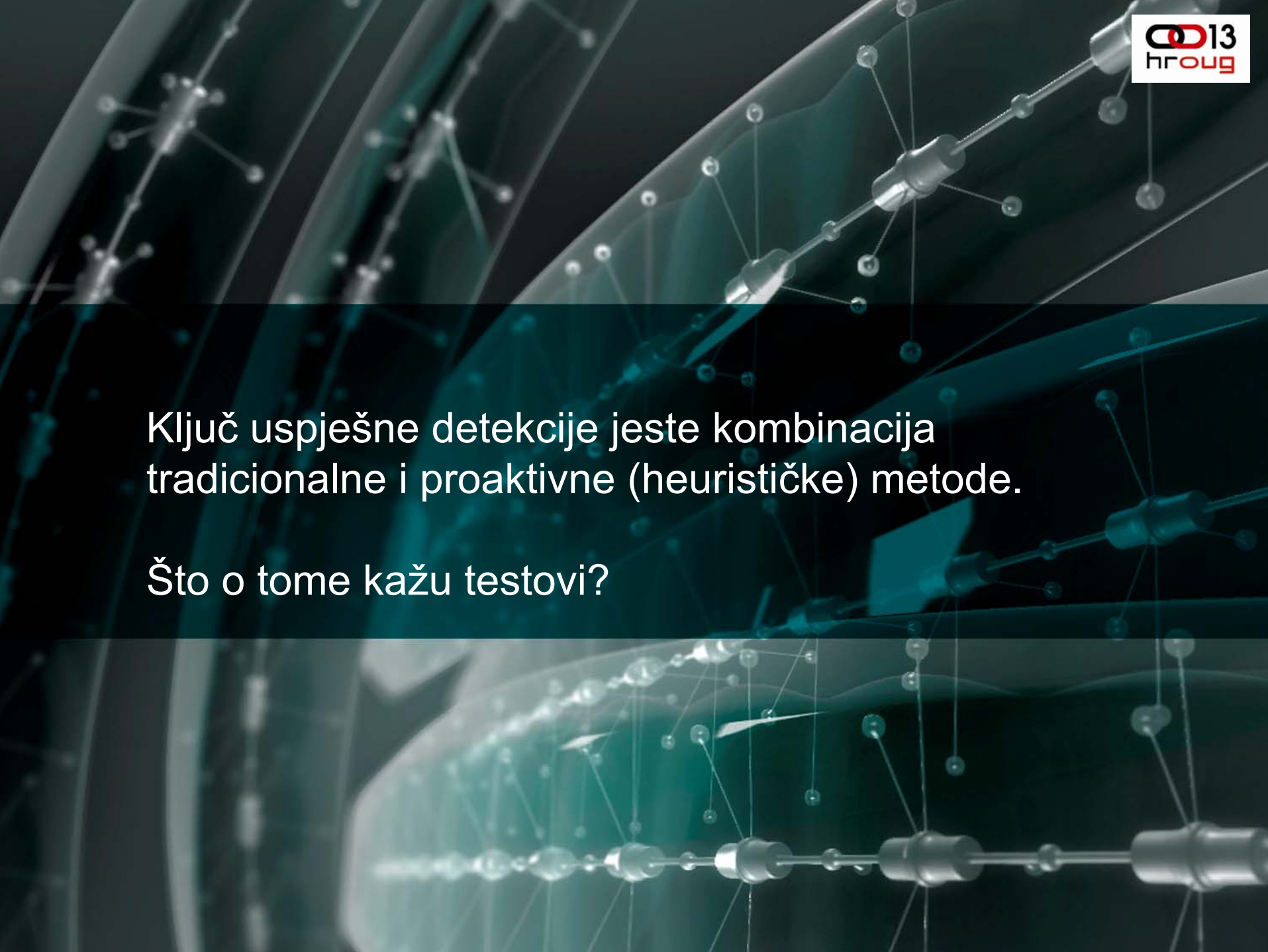
Proaktivna i tradicionalna detekcija



Heuristička detekcija



- Žuta linija pokazuje heurističku detekciju
- Bagle.CY je krenuo u 20:21UTC (i bio otkriven heuristički)
- Plava linija pokazuje točku definiranja specifične identifikacije Bagle.CY
- Klijenti koji nisu ažurirani još uvijek detektiraju heuristički


Ključ uspješne detekcije jeste kombinacija tradicionalne i proaktivne (heurističke) metode.
Što o tome kažu testovi?

Virus Bulletin testovi

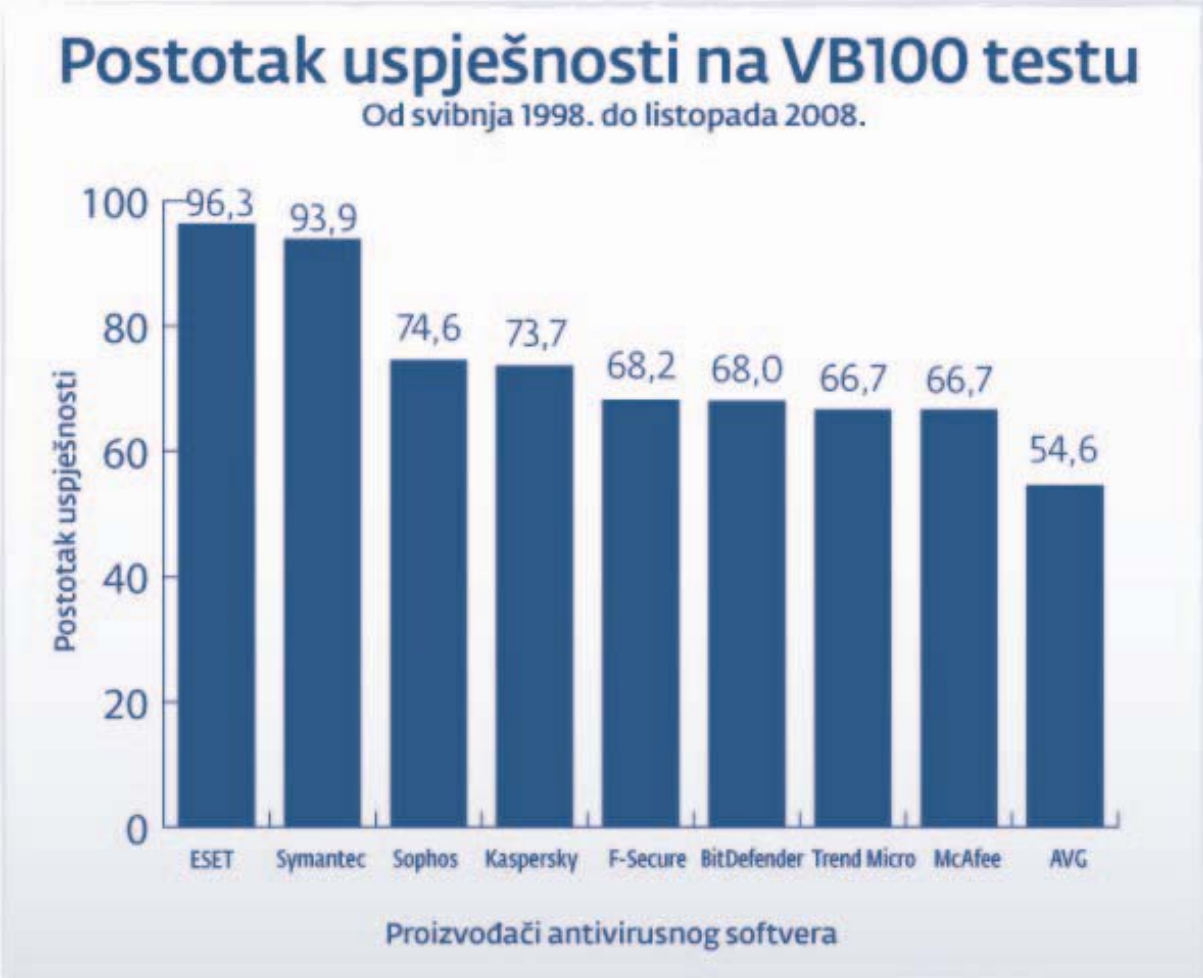
Virus Bulletin okuplja profesionalne, nezavisne antivirusne eksperte i najrespektabilnija je institucija u okvirima antivirusne industrije zbog kontinuiranog praćenja i izvođenja zahtjevnih komparativnih testova fokusiranih na detekciju, brzinu skeniranja i eventualno generiranje lažno pozitivnih detekcija (false postive). Za prolaz na testu i dobijanje Virus Bulletin 100% nagrade, antivirusni proizvod mora detektirati sve viruse ‘In the Wild’ kategorije bez ijedne ‘false positive’ detekcije.

NOD32 je jedino rješenje na svijetu koje nije propustilo detekciju “In the Wild” crva ili virusa na testiranjima od svibnja 1998. godine i drži rekord u broju osvojenih Virus Bulletin 100% nagrada. Zadnja, **52. po redu je osvojena u listopadu 2008.**

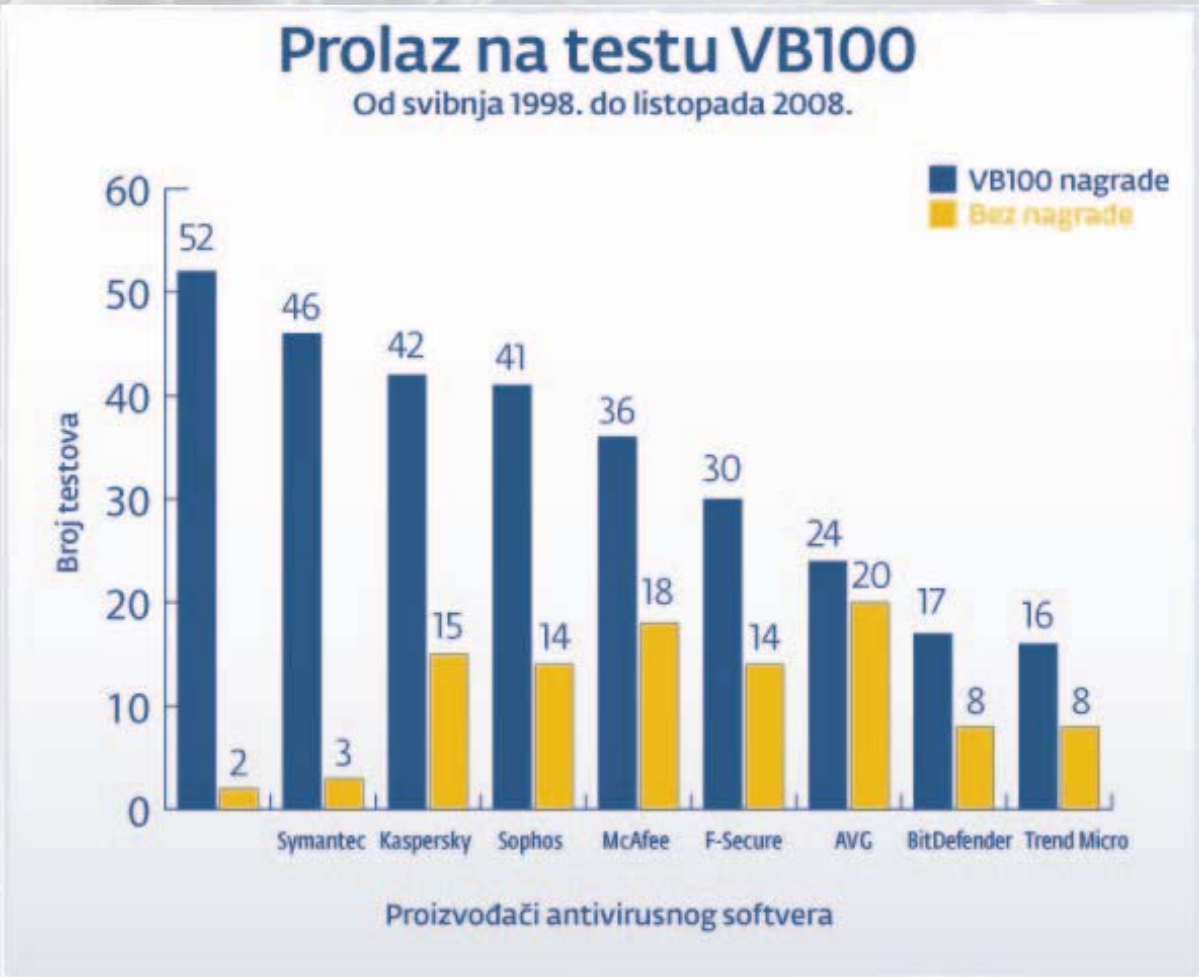
Virus Bulletin rezultati testiranja zadnjih 10 godina

Anti Virus Software Brand/Product	Times Tested Since May '98	Tests Failed	Tests Passed	Success Ratio %
NOD32 from ESET	**54**	**2**	**52**	**96.30%**
Symantec	49	3	46	93.87%
Microsoft OneCare (Since June '06)	4	1	3	75.00%
Sophos	55	14	41	74.55%
Kaspersky	57	15	42	73.68%
Norman	54	15	39	72.22%
CA eTrust	48	14	34	70.83%
Computer Associates (Vet)	34	10	24	70.59%
MicroWorld	23	7	16	69.57%
F-Secure	44	14	30	68.18%
BitDefender (SOFTWIN)	25	8	17	68.00%
Trend Micro	24	8	16	66.67%
McAfee	54	18	36	66.67%
GDATA	27	10	17	62.96%
FRISK	35	13	22	62.86%
Alwil (avast)	46	19	27	58.70%
H+BEDV	14	6	8	57.14%
Authentium	34	15	19	55.88%
VirusBuster	43	19	24	55.81%
AVG (Grisoft)	44	20	24	54.55%
Doctor Web	49	24	25	51.02%
GeCAD	23	17	6	26.09%
Panda	4	3	1	25.00%
Hauri	12	11	1	8.33%

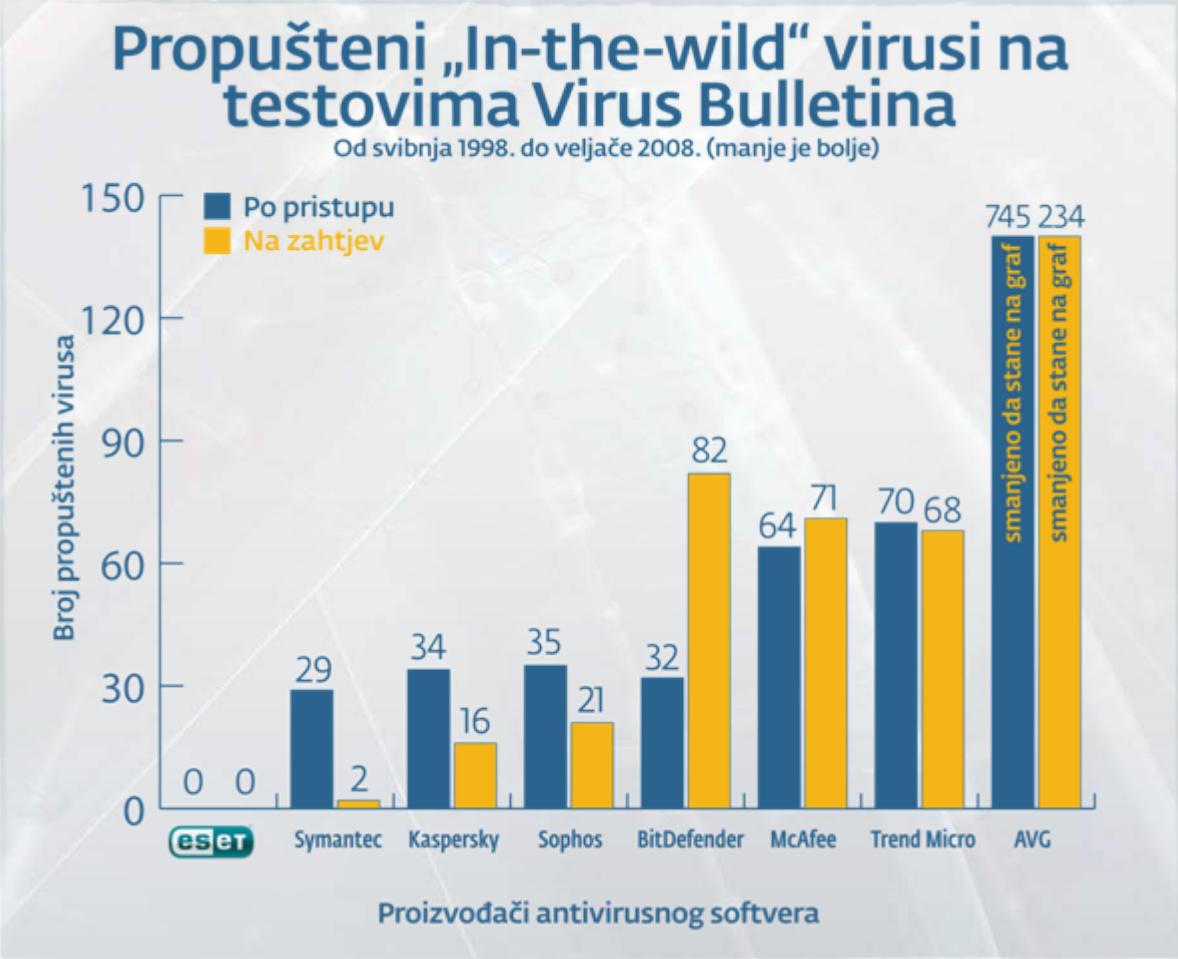
VB rezultati testiranja zadnjih 10 godina



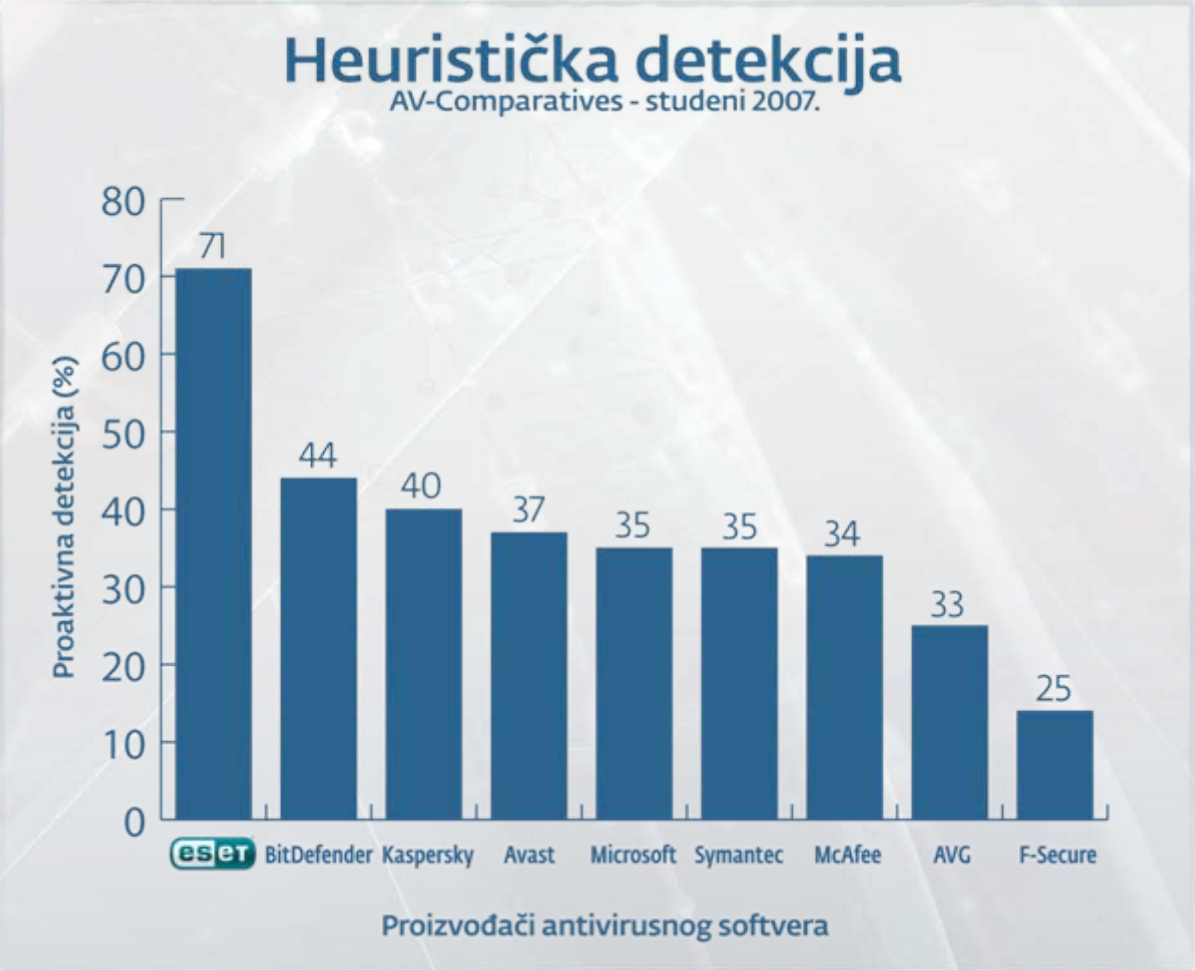
VB rezultati testiranja zadnjih 10 godina...



VB rezultati testiranja zadnjih 10 godina

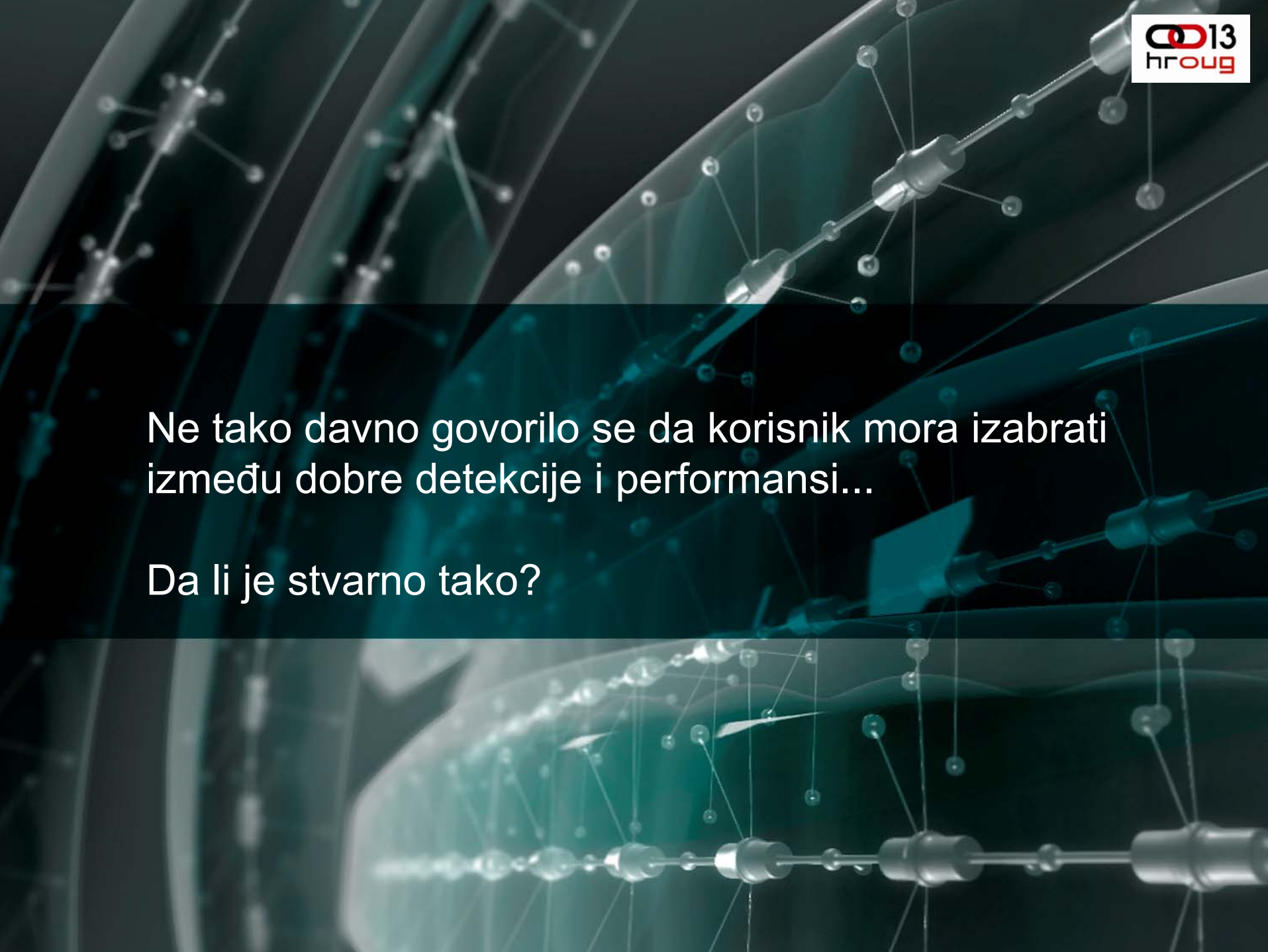


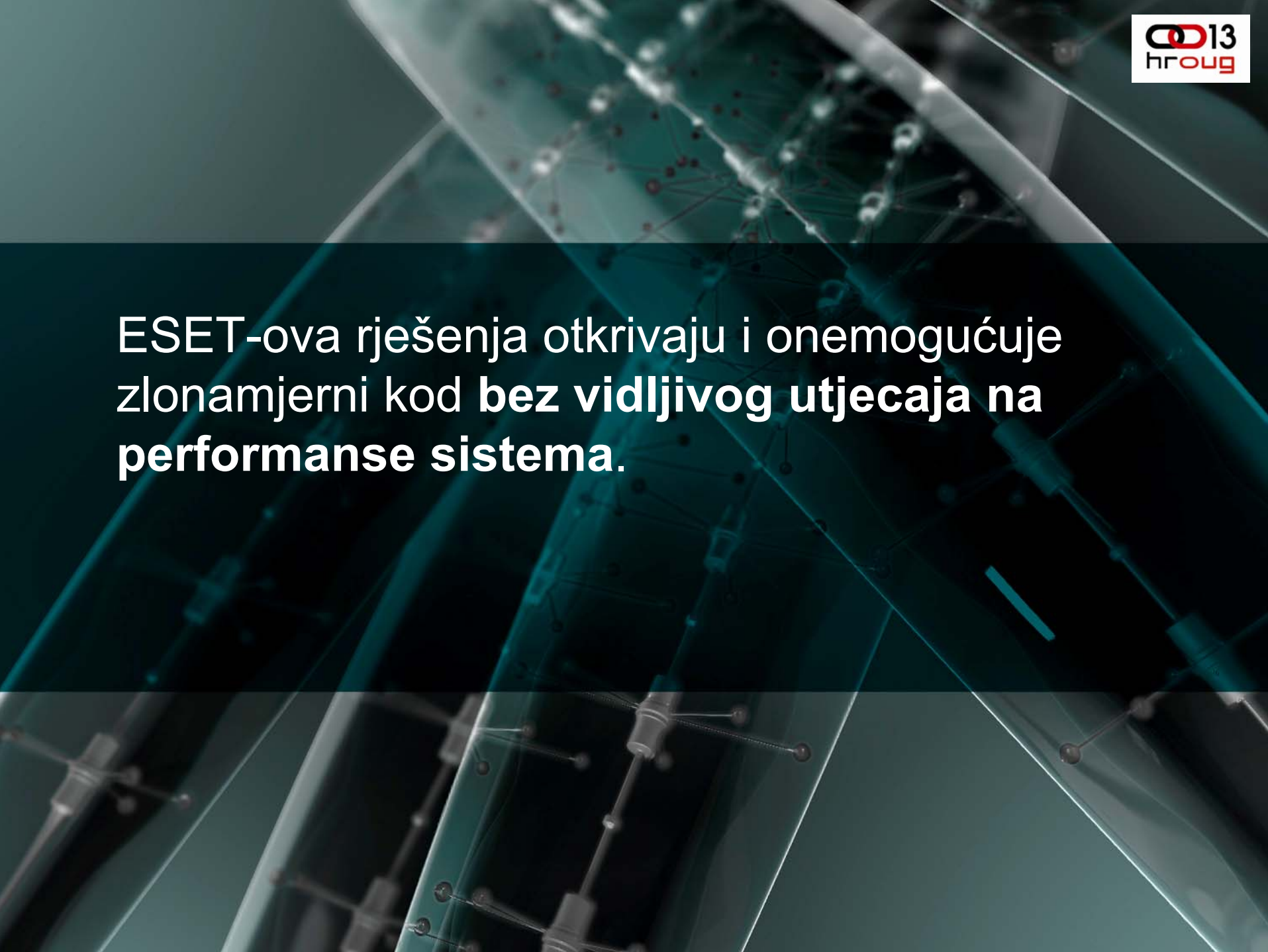
Rezultati testa proaktivne detekcije
Av-comparatives.org



Eset NOD32 Antivirus proglašen je ukupno najboljim antivirusnim rješenjem za **2006. i 2007. godinu** temeljem zbroja rezultata u tradicionalnoj i proaktivnoj detekciji.

www.av-comparatives.org


Ne tako davno govorilo se da korisnik mora izabrati između dobre detekcije i performansi...
Da li je stvarno tako?


ESET-ova rješenja otkrivaju i onemogućuje zlonamjerni kod **bez vidljivog utjecaja na performanse sistema**.

Performanse...

Prema rezultatima testova nezavisnih laboratorija, ESET NOD32 Antivirus i ESET Smart Security su jedna je od najbržih antivirusnih rješenja na tržištu, a zbog malih zahtjeva za resursima ne opterećuju računalo i ne usporavaju vas u svakodnevnom radu.

Citat iz izvještaja sveobuhvatnog uporednog testiranja performansi sprovedenog od strane West Coast Labs, objavljen 14.10.2008.:

Based upon the tests conducted on the specific versions during the test period, it can be seen that ESET had the lowest Commit Charge, and caused least delay to system and application start up times overall.

Testirani su McAfee Total Protection, Microsoft Forefront Client Security, Kaspersky Anti Virus 6.0 (with Kaspersky Administration Kit - free download), SOPHOS Endpoint Security 7.0 i Symantec Endpoint Protection 11.0.

Zainteresirani mogu pogledati cijeli izvještaj (33 stranice) na našem štandu.

Proizvodi

ESET NOD32 Antivirus

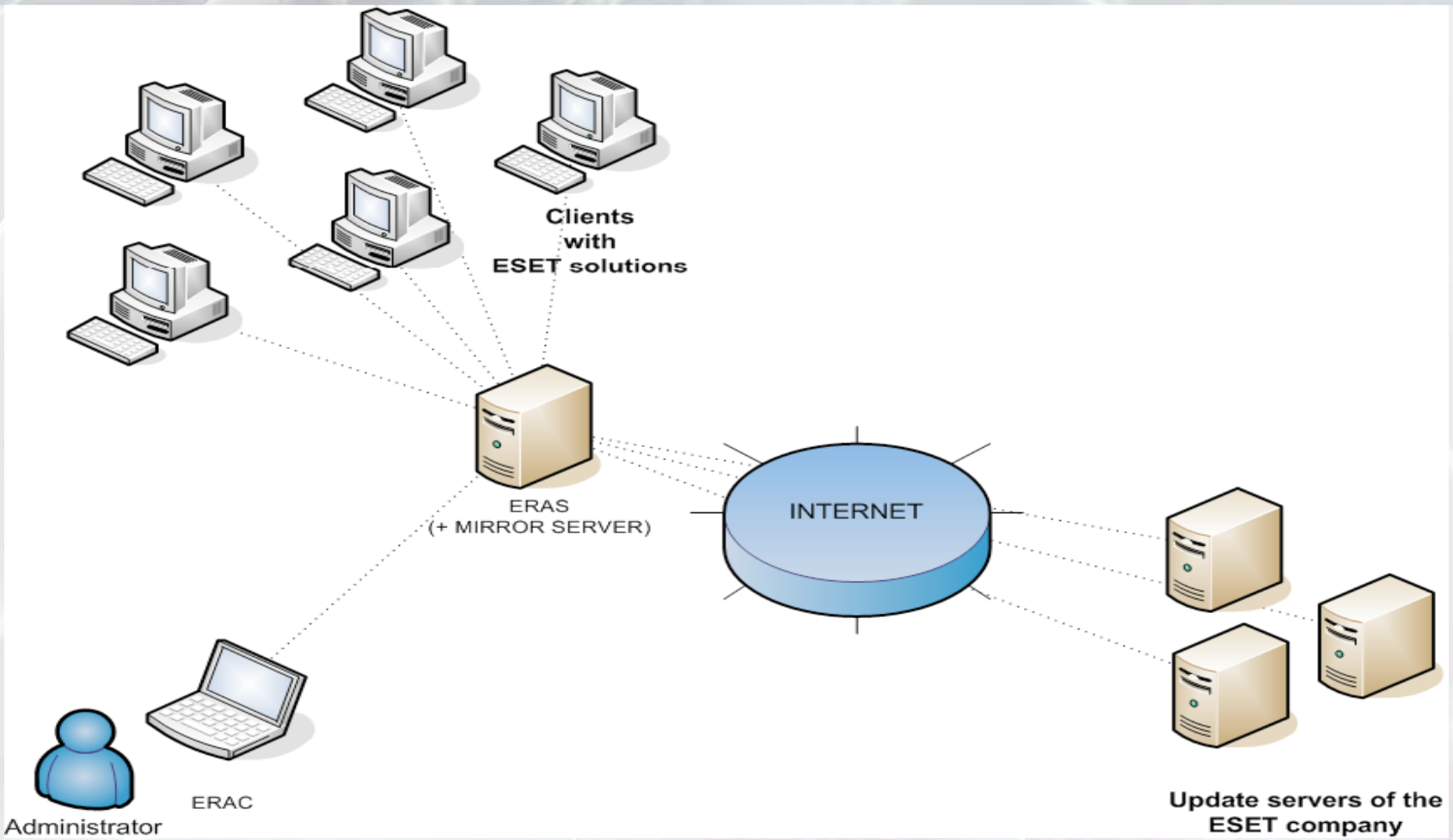
ESET NOD32 Antivirus Business Edition

Proizvodi

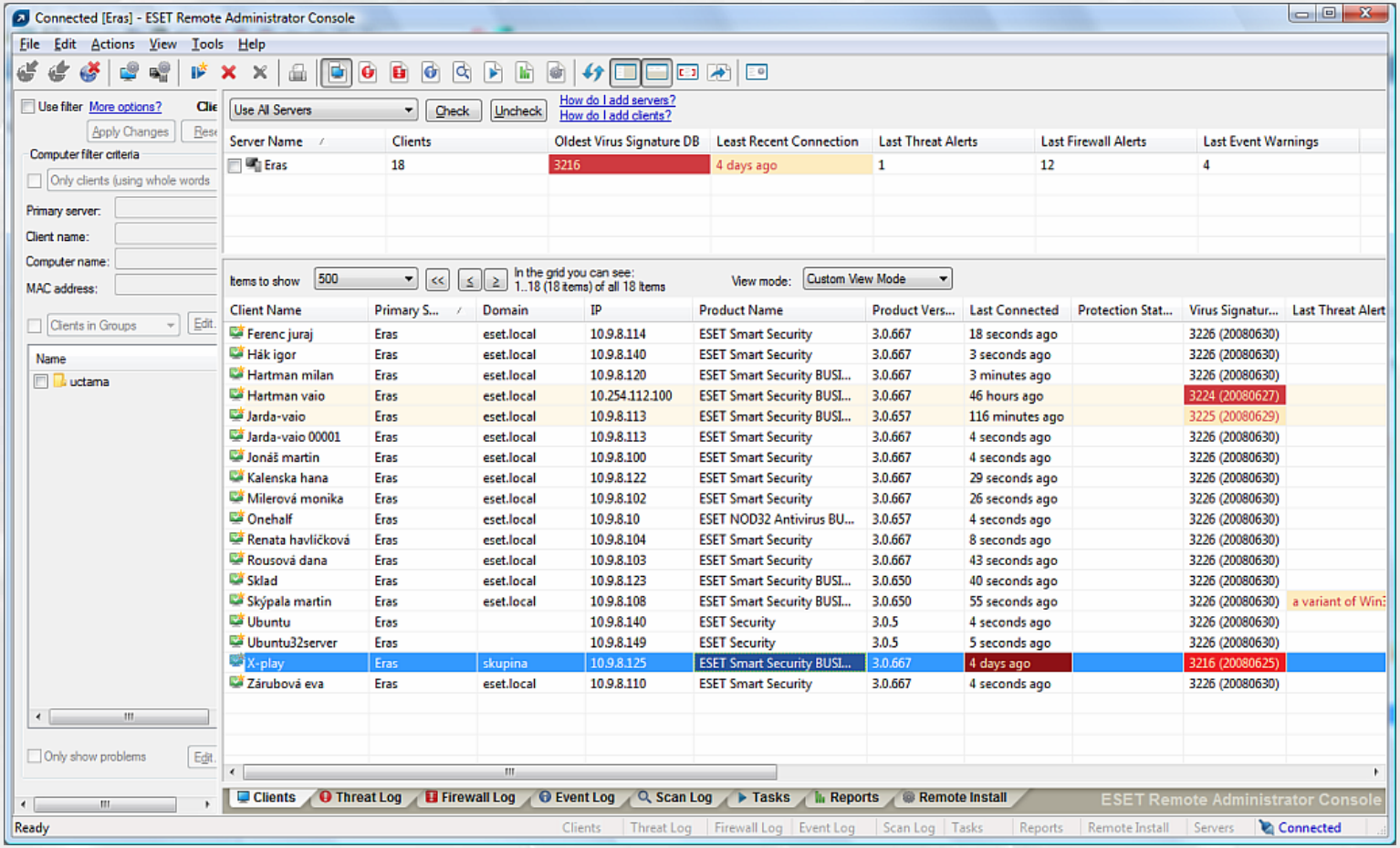
ESET Smart Security

ESET Smart Security Business Edition

ESET Business Edition (ERA)

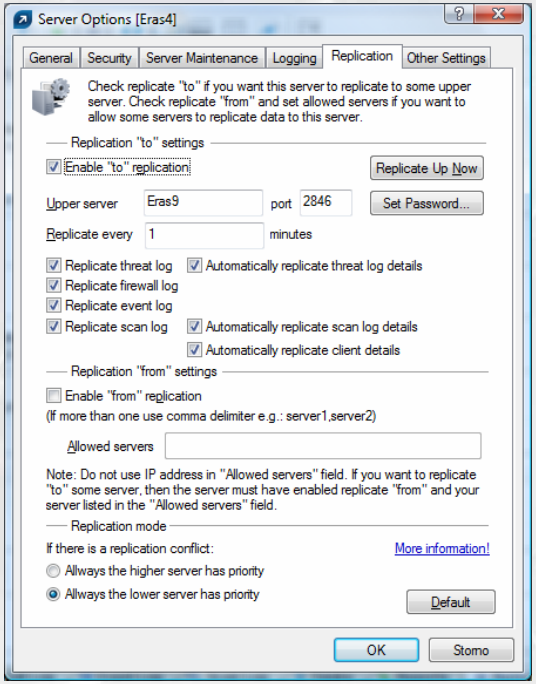


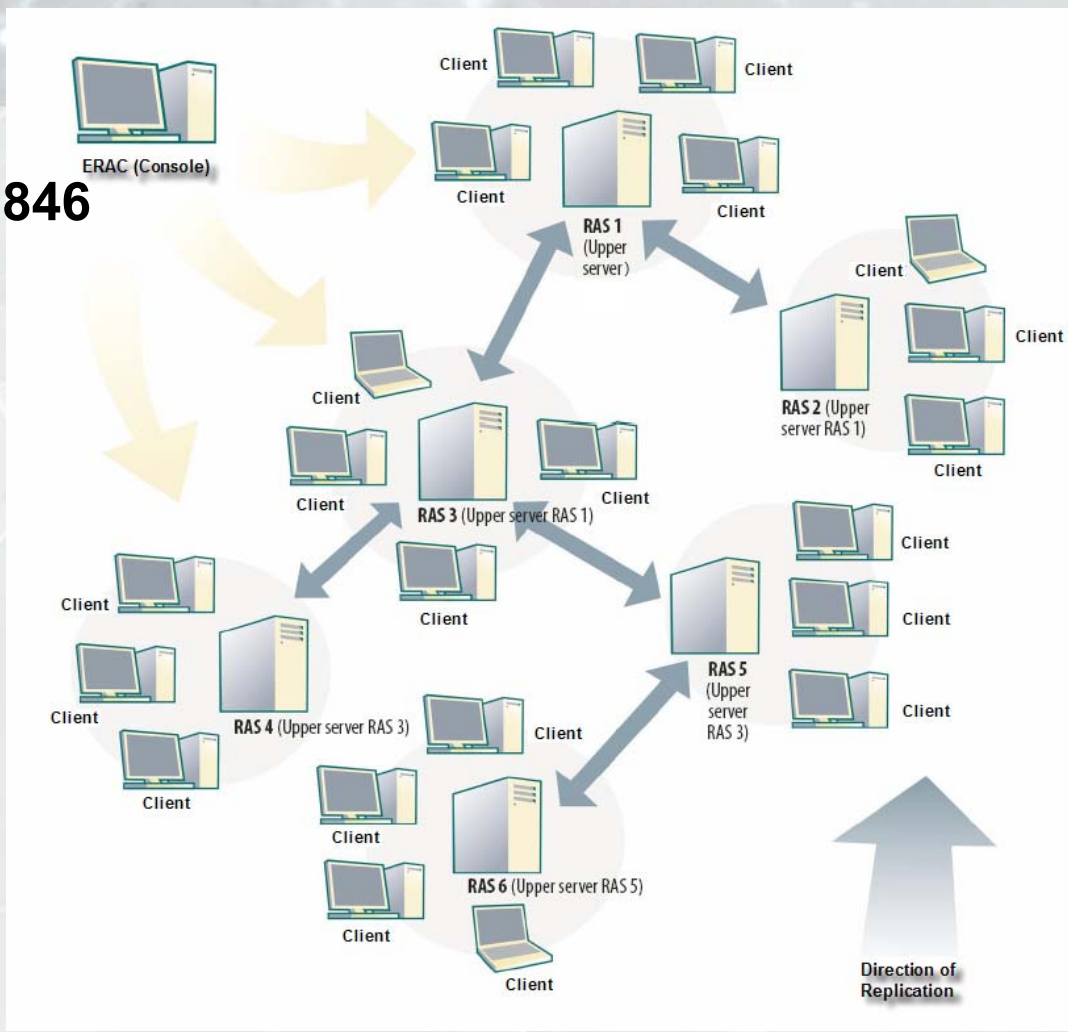
ESET Business Edition (ERA)



ESET Business Edition (ERA)

- **REPLIKACIJA**
  - **putem TCP porta 2846**





Proizvodi

ESET NOD32 for File Servers
- *Windows*
- *Linux*
- *Novell*

ESET NOD32 for Mail Servers
- *NOD32 for Exchange*
- *NOD32 for Linux Mail Server*
- *Lotus Domino*
- *Kerio Mail Server*

ESET NOD32 Gateway Security
- *Linux*

ESET NOD32 for
Kerio WinRoute Firewall
- *Windows*

Proizvodi

DELL™ Storage Servers (Windows Storage Server 2003)

Tako brz i malen da ćete jedva zamijetiti njegovu prisutnost...

Kako bi zaštitio svoje servere za pohranu podataka, Dell je odabrao NOD32. Dellov tim za tehničku evaluaciju izvršio je rigorozna testiranja više antivirusnih proizvoda. Nakon testiranja najpoznatijih antivirusnih brandova red je došao na NOD32. Instaliran je i pokrenut, ali kada aplikacija koja nadzire rad centralnog procesora nije pokazala promjenu u opterećenju centralnog procesora, zaključili su da NOD32 – ne radi. Podrobnija je analiza međutim pokazala kako NOD32 uistinu radi, ali opterećenje računalnih resursa od strane programa NOD32 bilo je ispod granične razine tolerancije aplikacije za nadgledanje performansi sustava!


Hvala na pažnji!
Pitanja?
www.eset.com.hr