

ESET – NEXT GENERATION

Filip Navrátil, Sales Engineer, ESET Software spol. s r.o.



we protect your digital worlds



Obsah

- Představení společnosti ESET
- Charakteristika současných infiltrací a trendy roku 2008
- Detekce hrozeb a technologie ThreatSense®
- ESET NEXT GENERATION
- Porovnání s konkurencí
- Dotazy

Představení společnosti ESET

- **ESET** vyvinul jeden z prvních antivirových produktů na světě
- Společnost ESET byla založena v roce **1992** v Bratislavě, SR
- **Produkty ESET jsou** hodnoceny jako jedny z **nejrychlejších** a **nejbezpečnějších** produktů na trhu. Důkazem je mnoho získaných ocenění.



- V současnosti je **centrála** společnosti **ESET** na Slovensku **v Bratislavě**, **pobočky** společnosti jsou **v Praze, Bristol, Buenos Aires, Krakow, San Diego** a zajišťuje **distribuci** produktů ve více než **160 zemích** po celém světě.



Charakteristika současných infiltrací

Charakteristika současných infiltrací

- Tvorba malware téměř výhradně za účelem výtěžku
 - Mnohdy je tvorba “na míru”
- Anonymita tvůrců
 - Bez touhy o jakoukoli medializaci (žádné „copyrighty“)
- Tvorba malware pod heslem „čas jsou peníze“
 - kvantita před kvalitou
 - žádné viditelné projevy, žádné destrukce

Trendy v roce 2008

- Falešné antivirus/antispyware produkty
- Programy pro zcizení účtů a hesel k online hrám
- Zneužívání funkce Autorun v systému Windows
- Zneužití datových formátů
- Pokračující "zero-day" útoky

Trendy v roce 2008

Antivirus XP 2008 | Your safe web-surfing solution

Full Windows XP Service Pack 3 Compatibility

Antivirus XP 2008

Scan your system for

• Pokraču

Antivirus XP 2008

Registration Support

Scan

System Status

Options

Update

About

Realtime Protection

Known viruses : 102563

Get Maximal Realtime Protection with Antivirus XP 2008

Buy

CZK 599.95 Pay by credit card

Antivirus XP 2008 Standard edition + 1 year free updates
Scanner + Spyware Remover + Real-Time Protection + bonus features
PRICE: CZK 599.95 (This is a One Time Only Charge, your credit card will never be rebilled and you will receive UPGRADES FOR FREE!)

CZK 1192 Pay by credit card

Antivirus XP 2008 Standard edition + 3 years free updates
Scanner + Spyware Remover + Real-Time Protection + bonus features
PRICE: CZK 1192 (This is a One Time Only Charge, your credit card will never be rebilled and you will receive UPGRADES FOR FREE!)

v bulletinu MS08-067

eků



Počet hrozeb a jejich variant je obrovský...
je nutné se efektivně bránit.

An abstract background featuring vibrant teal and blue light streaks and rays, creating a sense of motion and energy. The top half of the image is dominated by these dynamic light patterns, while the bottom half is a solid light gray.

Detekce hrozeb a technologie ThreatSense®

Detekce hrozeb a technologie ThreatSense®



- Technologie ThreatSense
 - Detekce širokého spektra hrozeb v jednom skenovacím jádru – adware, spyware, phishing, červi, viry, trojské koně, backdoory, rootkity, makroviry,...
- Proaktivní detekce i nových neznámých hrozeb
 - Exaktní detekce
 - Generická detekce
 - Heuristická analýza
 - Anti-stealth

Technologie ThreatSense.Net



- Automatický sběr dat o aktuálních a nových hrozbách detekovaných produkty ESET.
- Data jsou automaticky zasílána na analýzu do virových laboratoří.
- Díky unikátní heuristické analýze umožňuje technologie ThreatSense.Net rychlou analýzu a reakci na nové hrozby.
- Poskytuje přesné informace o šíření jednotlivých hrozeb.



Produktové portfolio ESET

ESET Produktové portfolio

- Ochrana stanic
- Ochrana mobilních zařízení
- Centrální správa
- Ochrana souborových serverů
- Ochrana poštovních serverů
- Ochrana gateway





Ochrana stanic

Ochrana stanic

- ESET Smart Security 4
 - Anti-virus, Anti-spyware, Firewall , Anti-spam



- ESET NOD32 Antivirus 4
 - Anti-virus, Anti-spyware



ESET Smart Security 4 Business Edition

Hlavní výhody

- Využitím **ThreatSense** technologie je zajištěna maximální **ochrana proti známým i neznámým hrozbám**
- Extrémně **nízké systémové nároky**
- Vynikají **rychlost skenování**

ESET Smart Security 4 Business Edition

Nov

• Se

• O

• Int

• P

• Oc

• O

• Oc

• K

• Po



ESET Smart Security 4 Business Edition

Nové vlastnosti a vylepšení

- Kontrola přístupu k výměnným médiím
- Rozšířená podpora e-mailových klientů
- ESET SysRescue - záchranné CD/USB
- Kontrola šifrované komunikace a „učící se“ režim
- Podpora přenosných počítačů

ESET Smart Security 4 Business Edition

Nové vlastnosti a vylepšení

- Funkce Mirror

- Funkce Mirror zajišťuje centralizované aktualizace produktů ESET ve firemním prostředí, snižuje objem přenášených dat z internetu a přes VPN linky.

- Centrální správa pomocí ESET Remote Administrator

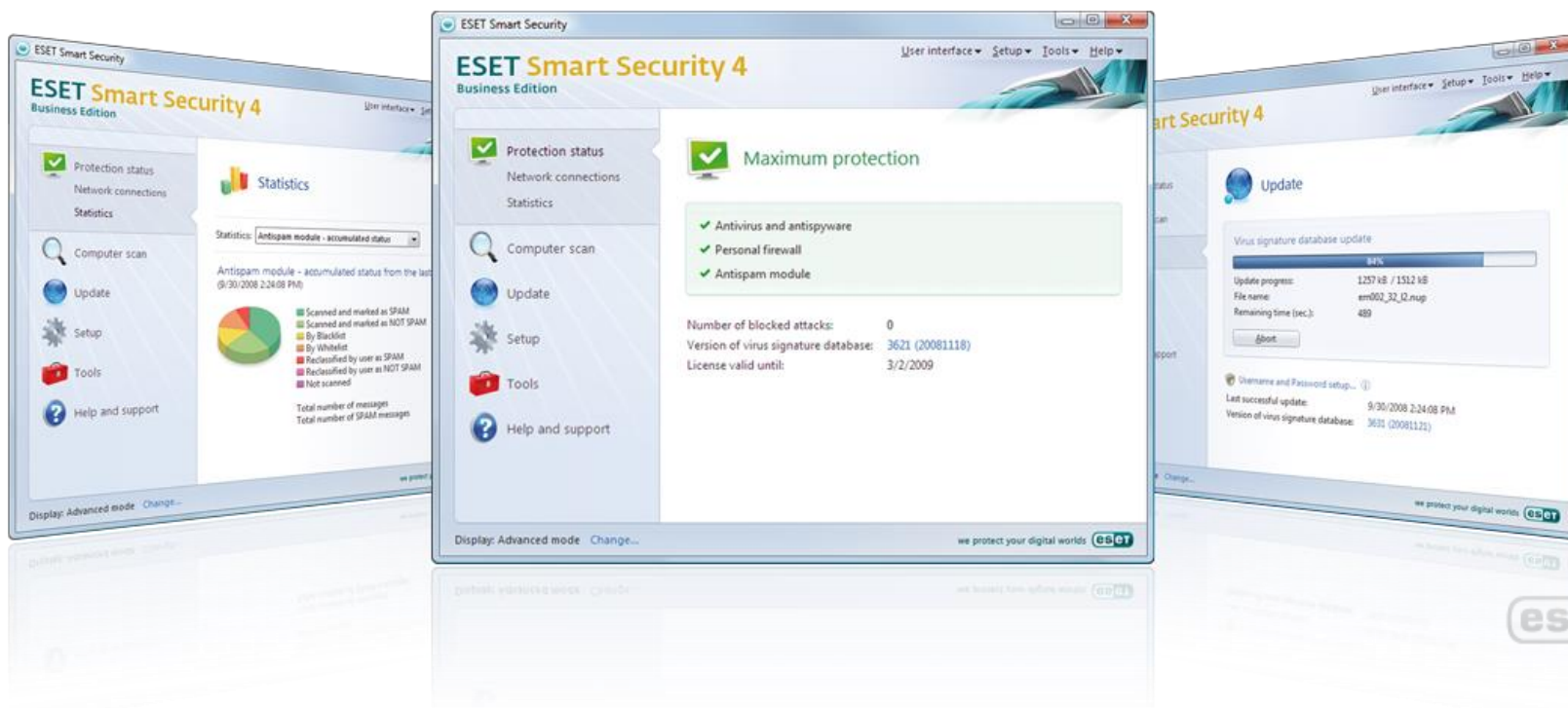
- ESET Remote Administrator 3 zajišťuje centrální správu produktů ESET, umožňuje tak správu a monitoring bezpečnostních produktů kdekoli a kdykoli.



ESET Smart Security 4 Business Edition

Nové vlastnosti a vylepšení

- Uživatelské rozhraní
 - Nové vylepšené grafické uživatelské rozhraní obsahuje grafy a statistické informace o činnosti jednotlivých komponent.
 - Pokročilým uživatelům/administrátorům je k dispozici rozšířené nastavení.

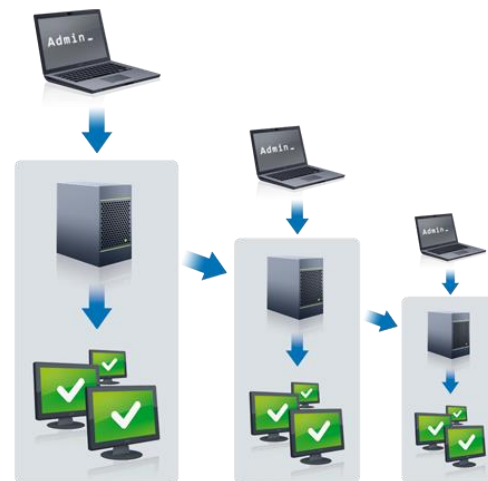




Centrální správa – ESET Remote Administrator

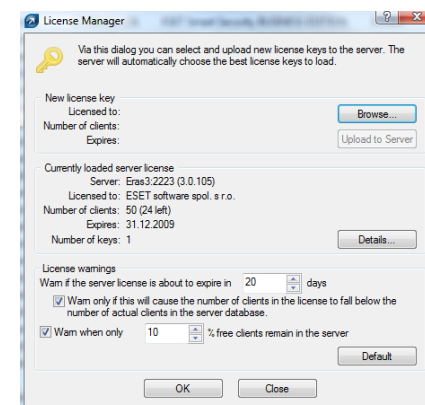
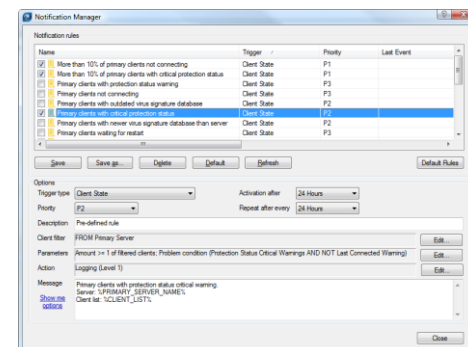
Centrální správa – ESET Remote Administrator

- Možnost hierarchické správy více RA serverů s replikací
- Synchronizace s Active Directory
- Nová správa politik klientů
 - hierarchická stromová struktura politik
 - možnosti použití fragmentů konfigurace, více typu dědění
 - pravidla pro automatizované přidělování politik
 - široce konfigurovatelné podmínky, možnost aplikovat i na požádání



Centrální správa – ESET Remote Administrator

- Notification Manager
 - Upozornění generované na základě událostí
 - Filtr klientů, možnost volby několika akcí
- Funkce Mirror (součástí stanicových produktů)
 - Centrální distribuce aktualizací v organizaci
- Read-Only přístup přes konzoli
- Správa licencí
- Vylepšená škálovatelnost přenosu dat



Centrální správa – ESET Remote Administrator

Systémové požadavky:

- **ESET Remote Administrator Console**

- Operační systém: Microsoft Windows 2000/XP/2003/2008/Vista
- Internet Explorer: minimum 4.0, doporučená verze 5.5

- **ESET Remote Administrator Server**

- Operační systém: Microsoft Windows NT4 (Service Pack 6)
2000/XP/2003/2008/Vista
- Internet Explorer: minimum 4.0, doporučená verze 5.5

- **Databáze**

- MySQL 5.0, ORACLE 9i, MS SQL 2005



Ochrana mobilních zařízení

Ochrana mobilních zařízení

ESET Mobile Antivirus

- Proaktivní detekce
 - Využívá heuristickou analýzu upravenou pro použití na mobilních zařízeních
- SMS Antispam
- Rozšířené možnosti skenování
 - Kontrola integrované paměti, výměnných paměťových karet, běžících procesů, příchozích a odchozích souborů, komprimovaných (cab) souborů.
- Automatické aktualizace
 - Automatické aktualizace s možností plánování.





Ochrana souborových serverů

Ochrana souborových serverů

Podporované platformy:

- ESET NOD32 Antivirus pro MS Windows File Server
- ESET File Security pro Linux/BSD
- ESET NOD32 Antivirus pro Novell Netware

Ochrana souborových serverů – společné vlastnosti

- Využití **ThreatSense** technologie je zajištěna maximální **ochrana proti známým i neznámým hrozbám**
- Extrémně **nízké systémové nároky**
- Vynikají **rychlost skenování**
- **On-Access, On-Demand kontrola** (včetně FTP, Samba)
- Podpora aplikace **ESET Remote Administrator**
- Podpora **32/64-bit systémů**



Ochrana poštovních serverů

Ochrana poštovních serverů

Podporované platformy:

- ESET Mail Security pro Linux/BSD/Solaris
- ESET NOD32 Antivirus pro MS Exchange
- ESET NOD32 Antivirus pro Lotus Domino
- ESET NOD32 Antivirus pro Kerio Mail Server

Ochrana poštovních serverů – společné vlastnosti

- **Ochrana před viry a spyware**
 - Technologie ThreatSense® ve verzi 3.0
- **Kontrola protokolů SMTP (POP3 a IMAP)**
- **Spamový filtr**
 - Funkce „net-check“ zaručuje rychlejší a kvalitnější detekci nevyžádané pošty
- **Rozšířená podpora agentů a platforem**
 - kompatibilní s nejrozšířenějšími MTA (Postfix, Sendmail, Qmail, Exim,...)
- Podpora **32/64-bitových** systémů
- Podpora aplikace **ESET Remote Administrator**



Ochrana gateway serverů

Ochrana gateway serverů

Podporované platformy:

- ESET Gateway Security pro Linux/BSD/Solaris
- Kerio Winroute Firewall

ESET Gateway Security pro Linux/BSD/Solaris - klíčové funkce

- Skenování **transparentními proxy** moduly
 - pracuje jako **transparentní HTTP/FTP proxy server**
 - Lze nasadit jako **plug-in pro SafeSquid Proxy Cache**
- **Technologie částečného skenování**
 - bezpečná a rychlá kontrola velkých HTTP downloadů
- Rozšířená podpora platforem a systémů
 - Linux, FreeBSD, NetBSD a Sun Solaris, 32/64-bitové systémy
- Podpora aplikace **ESET Remote Administrator**



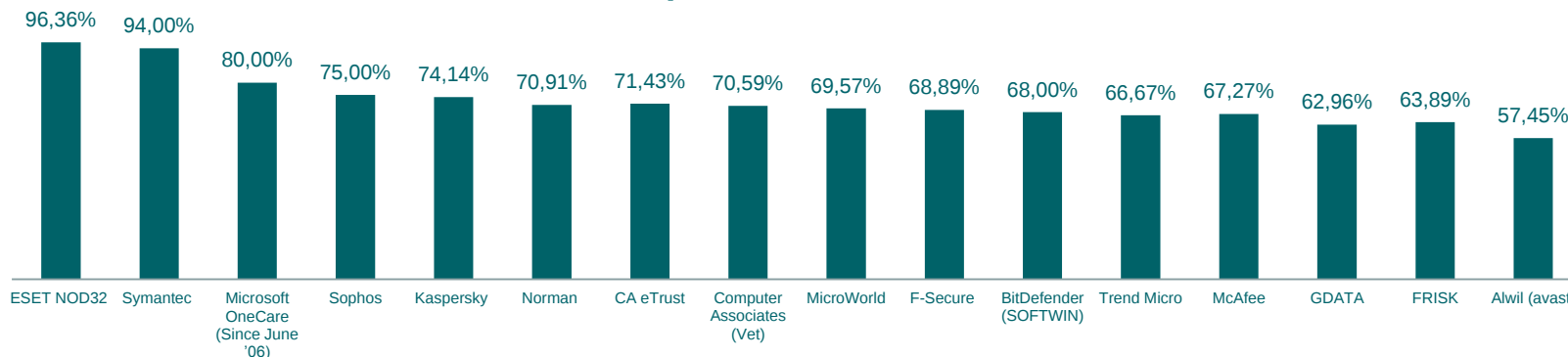
Porovnání s konkurencí

Proč řešení ESET?

Ocenění

NOD32 je jediné řešení na světě, které od května 1998 nikdy neminulo ani jedinou hrozbu “In the Wild” a drží rekord v počtu ocenění VB100. V prosinci 2008 získalo řešení NOD32 již 53 ocenění VB100 a je dle Virus Bulletinu hodnoceno jako neoceňovanější a nejúspěšnější antivirový produkt.

Úspěšnost testů v %



Virus Bulletin

is an independent testing organization with full time professional, independent antivirus experts. VB is widely recognized within the antivirus industry for their rigorous comparative tests focusing on virus detection rates, scanning speed, and generation of false positives. To earn a Virus Bulletin Award (VB100), an antivirus product must detect all of the current “In the Wild” viruses and not produce any false positives.

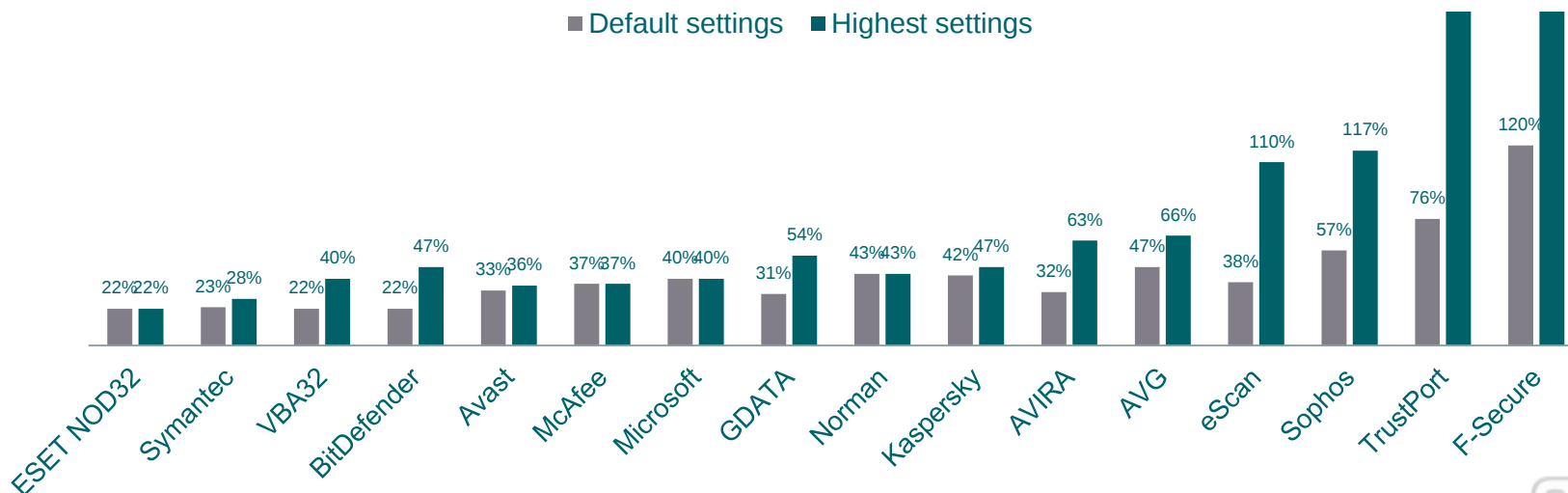
Proč řešení ESET?

VÝKON A RYCHLOST

- Je váš počítač pomalý? Potřebujete rychlejší bezpečnostní řešení s nízkými nároky?
- **ESET verze 4 má nejrychlejší start počítače ze všech testovaných produktů**
(AV-comparatives.org; October 2008)
- **Nejmenší systémové nároky a vliv na rychlost systému**
(overall performance test winner 2008, AV-comparatives.org)

Celkový vliv na systém v %

■ Default settings ■ Highest settings



Děkuji za pozornost.

Filip Navrátil, Sales Engineer, ESET Software spol. s r.o.

