Ať se stane cokoliv...

Konvergence bezpečnosti a dostupnosti

Radek Smolík
Country Manager
Symantec ČR a SR

Obraz reálných zkušeností...

Wednesday, January 19 12:00 AM ET

Microsoft's AntiSpyware Tool Removes Internet Explorer

By Brian Briggs

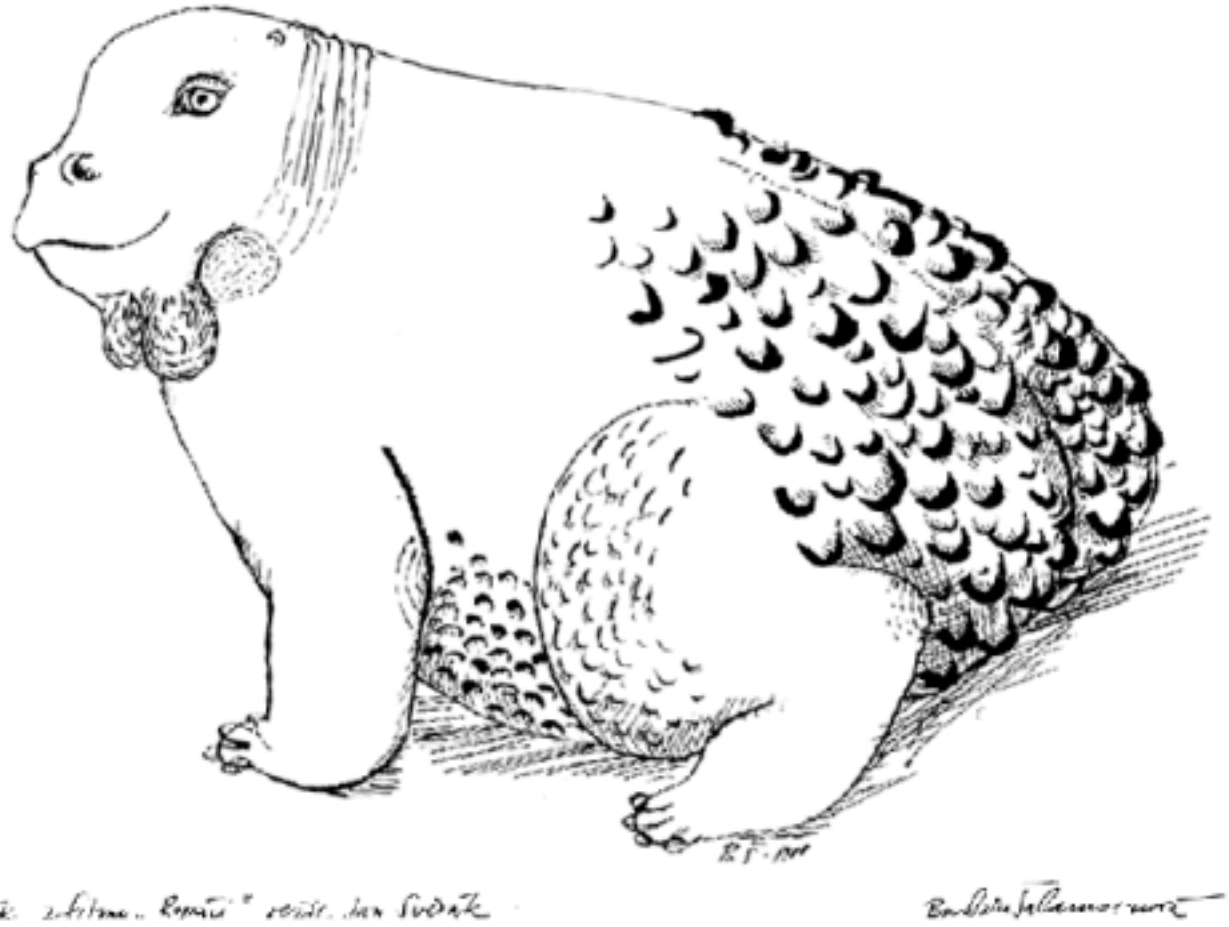
Many Microsoft Windows users who downloaded the rec
AntiSpyware program from Microsoft, or had it installed
automatic Windows update, woke up to a surprise. Unin
heuristics of the software detected Internet Explorer as
removed the program from their systems.

Microsoft ha
program fro
until the prol
corrected. E
Weatherbee
representati
program wa
and that "a f
forthcoming.

"It shows ho
AntiSpyware program is," said Weatherbee. "Not only is
remove spyware from the system, but also the source of
Our competitors can't match that."

symantec.

Copak je to za „zvířátko“?



Znáte tohle zvíře?

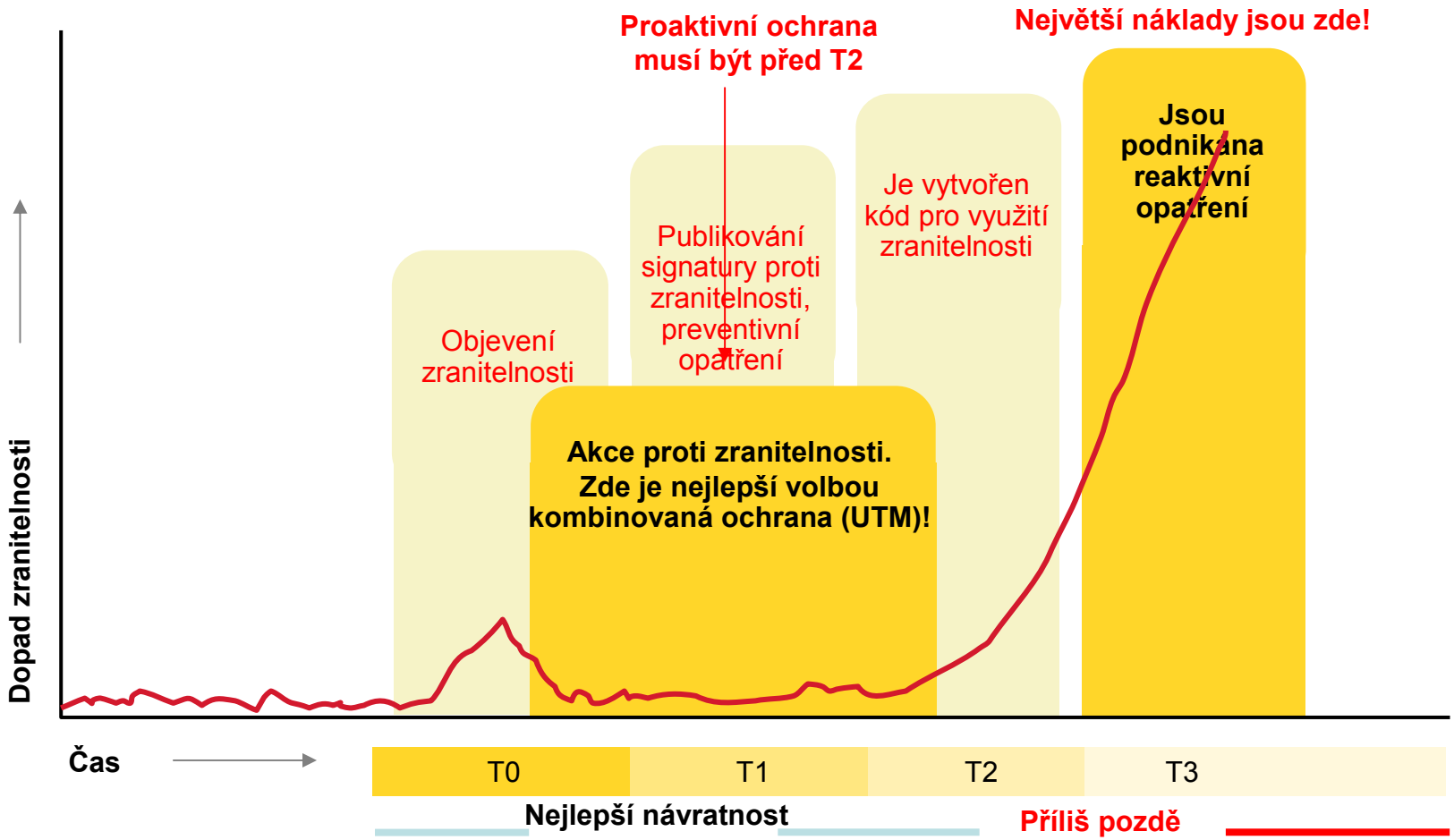
Udržíme Vás na nohou, v chodu a rostoucí, ať se stane cokoliv !

Kdo by rád dělal tuhle práci?

Nebojte se, s námi se Vám nic nestane!

Bojte se, co všechno by se Vám mohlo stát bez nás!

Odpovědi na zranitelnosti



Příklad první - proaktivní bezpečnost (v Čase 0)

- Proaktivní prevence před novými a neznámými hrozbami
  - Zastavení hrozeb PŘEDTÍM, než vůbec vstoupí do sítě
  - Zastavení převážné většiny neznámých hrozeb v „by default“ konfiguraci a bez nutnosti reaktivních aktualizací

Symantec Gateway Security již chránila před následujícími hrozbami. ***MODRÉ*** *položky* byly zastaveny bez nových signatur, definic nebo zásahu obsluhy !!!

„By default“ ochrana proti:

Application-layer attacks
WebDAV Buffer Overflow
SENDMAIL
Code Red /Code Red II
FTP Bounce
NIMDA
W32.SQLExp.worm (SQL Slammer Worm)
FTP Buffer Overflow
HTTP Buffer Overflow
NNTP Buffer Overflow
WINS Buffer Overflow
HTTP Directory Transversal
Blaster
Welchia

Denial of Service Attacks (DoS)
Syn Flooding
Syn-Ack Attack
Jolt, Jolt2
Shaft
Mstream
Ping of Death
Bonk
Trex
KKill
Octopus
Novarg, (aka: Mydoom)

Distributed Denial of Service (DDoS)
Port Scanning Attack
Ping Flooding Attack
SYN Flooding Attack
Syn-Ack Attack
TCP Sequence Prediction Attack
DNS Cache Poisoning
SNMP Attack
Tribe/Trinoo/TFN2k/Stacheldracht
IP Fragmentation/Overlapping Fragment Attack (Teardrop, Unnamed)
Stream3
Smack
Overlap

*Blue = ochrana bez akce administrátora nebo aktualizace
Black = ochrana, po akci administrátora

24 po sobě jdoucích 100%-ních detekcí

Date	Pro	Symantec	Symantec	Trend	Sophos	McAfee	Kaspersky	GeCAD RAV	CA Vet	CA eTrust	F-secure
Dec-05	Windows Se	PASS	PASS	-	-	PASS	PASS	-	PASS	-	-
Oct-05	Windows 1	PASS	PASS	PASS	PASS	PASS	PASS	-	PASS	PASS	PASS
Jun-05	Windo	PASS	PASS	-	PASS	PASS	PASS	-	PASS	PASS	PASS
Feb-05	Windo	PASS	PASS	-	PASS	FAIL	PASS	-	PASS	PASS	FAIL
Nov-04	Windows 1	PASS	PASS	PASS	PASS	PASS	PASS	-	FAIL	FAIL	PASS
Aug-04	Net	PASS	PASS	-	PASS	PASS	PASS	-	PASS	PASS	-
Jun-04	Windows XI	PASS	PASS	-	PASS	PASS	PASS	-	PASS	PASS	PASS
Feb-04	Windo	PASS	PASS	PASS	PASS	PASS	PASS	-	PASS	PASS	PASS
Nov-03	Windows 1	PASS	PASS	PASS	PASS	PASS	PASS	-	PASS	FAIL	PASS
Aug-03	Netw	PASS	PASS	-	PASS	PASS	PASS	-	PASS	FAIL	-
Jun-03	Windows XI	PASS	PASS	PASS	PASS	PASS	FAIL	PASS	PASS	PASS	PASS
Feb-03	Windo	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Nov-02	Windo	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Jun-02	Windo	PASS	PASS	FAIL	PASS	PASS	FAIL	PASS	PASS	PASS	PASS
Feb-02	Windo	PASS	PASS	PASS	PASS	-	FAIL	FAIL	PASS	FAIL	FAIL
Nov-01	Windo	PASS	PASS	PASS	PASS	FAIL	PASS	FAIL	PASS	PASS	FAIL
Apr-01	Windo	PASS	PASS	-	PASS	PASS	FAIL	FAIL	PASS	PASS	FAIL
Feb-01	Windo	PASS	PASS	-	FAIL	FAIL	FAIL	FAIL	PASS	FAIL	-
Nov-00	Windo	PASS	PASS	-	FAIL	FAIL	FAIL	FAIL	PASS	PASS	FAIL
Sep-00	Net	PASS	PASS	-	PASS	FAIL	FAIL	FAIL	PASS	PASS	-
Jul-00	Windo	PASS	PASS	-	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL	FAIL
Apr-00	Windo	PASS	PASS	-	PASS	FAIL	PASS	FAIL	PASS	FAIL	PASS
Feb-00	D	PASS	PASS	-	PASS	PASS	PASS	FAIL	PASS	-	FAIL
Nov-99	Windo	PASS	PASS	-	FAIL	FAIL	PASS	PASS	PASS	FAIL	FAIL
		PASS									
PASS		PASS	24	9	19	15	16	5	22	14	11
FAIL		PASS	0	1	4	8	8	9	2	8	8
		PASS									
		PASS									
		24									
		0									

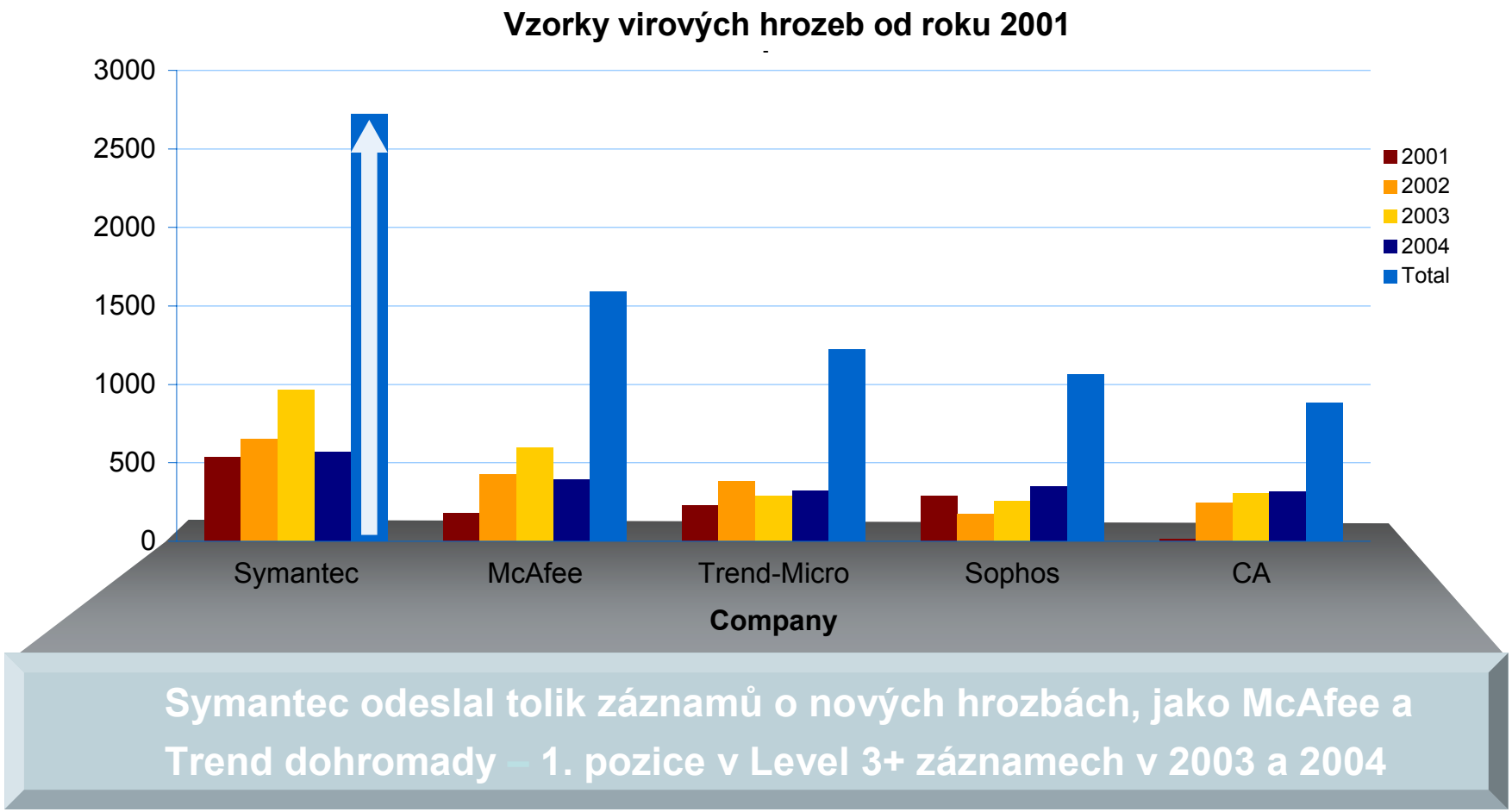
Symantec:

- ***Hotové testy pro všechny testované O/S od listopadu 1999***
- ***JEDINÝ dodavadatel, který získal 24 po VB100***

- **Pass:** Detected all "In the Wild viruses" in comparative tests (with no false positives)
- **Fail:** Missed detection after three attempts
- **—**: Chose not to submit for testing

Udržíme Vás na nohou, v chodu a rostoucí, ať se stane cokoliv !

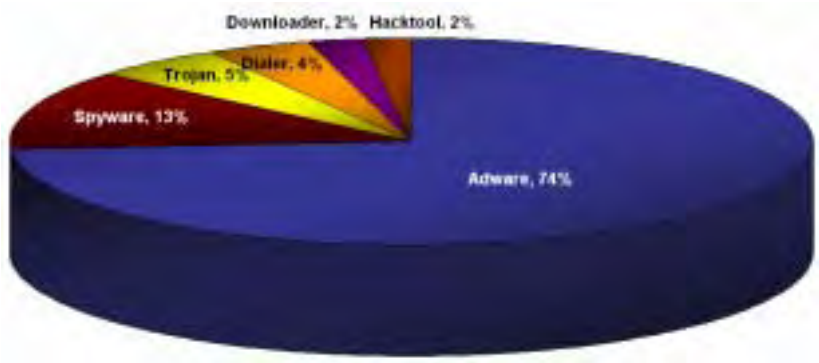
Systém včasného varování se vyplácí



Symantec odeslal tolik záznamů o nových hrozbách, jako McAfee a Trend dohromady – 1. pozice v Level 3+ záznamech v 2003 a 2004

Stav rozvoje spyware

- Symantec obdrží týdně přibližně 20.000 - 25.000 zásilek nových hrozeb. Procentuální podíl spyware v nich stále roste
- Adware nyní tvoří plných 7% z TOP10 typů hrozeb, které zaznamenáváme
- V průběhu rutinního testování “živých” zdrojů vidíme lví podíl spyware na zjištěných kompromitacích
  - Souběh spyware a trojské logiky je velmi častý
- Vážné dopady: obecně odhadujeme, že spyware „stojí za“ ~20% zásahů helpdesku



Rank	Program name
1	ShopAtHomeAgent
2	Istbar
3	CoolWebSearch
4	SearchAssistant
5	Iefeats
6	Gain
7	BetterInternet
8	VirtuMonde
9	EliteBar
10	NdotNet

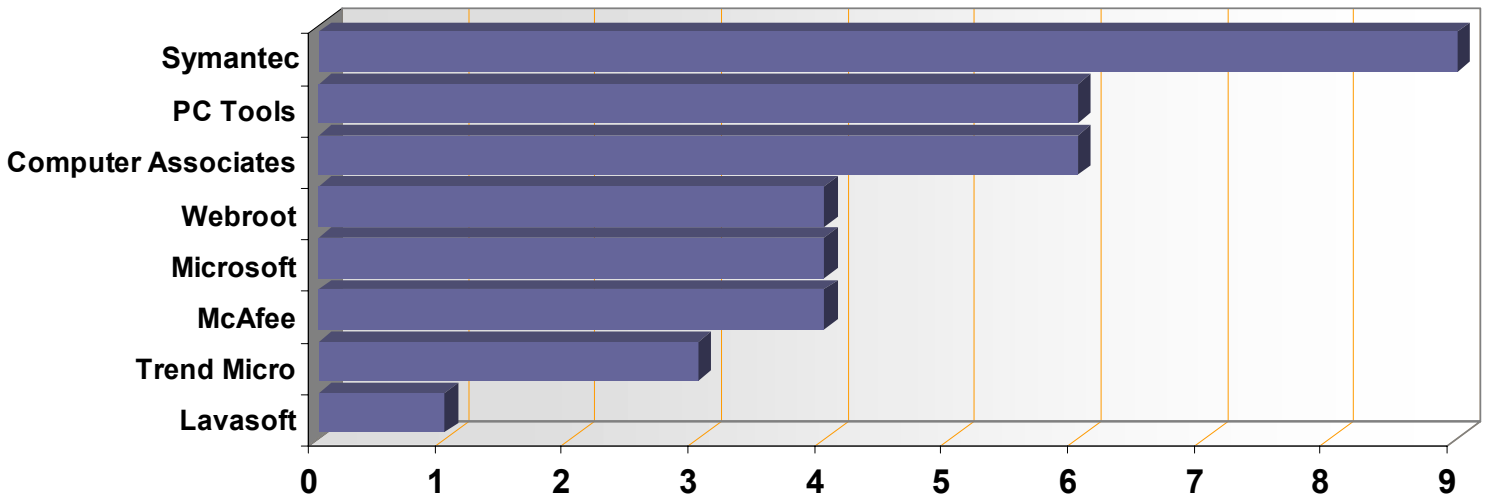
Zdroj: Symantec’s Internet Security Threat Report September 2005 for 6 month period July-December 2005

Rozhoduje přesnost a spolehlivost

ZiffDavis Editor's Choice

"Symantec… zazářil na poli detekce, což je tím, co si chcete pořizovat..."

ZiffDavis – Porovnání přesnosti detekce



http://www.zdnet.com.au/reviews/software/security/soa/To_catch_a_spy_Eight_anti_spyware_tools_reviewed/0,39023452,39225147,00.htm

Ale ani to nestačí. Co kdybychom uměli...?

- Vytvoření klonovacího image systému v reakci na zjištění nové zranitelnosti nebo útoku proti ní...
- Detekovat nebezpečné kódy bez definic či signatur či automaticky odpojit napadené počítače od vybraných služeb sítě...
- Provést zálohu dat a aplikací na základě zjištěného dění na firewallech a IPS...
- Vytvářet incidenty nejen z logu bezpečnostních systémů, ale i z provozních stavů - zálohy, chod clusterů, ztráty paketů...
- Replikovat kritické aplikace a jejich data mezi lokalitami, aktivovat v případě napadení či výpadku části...
- A mnoho dalšího...

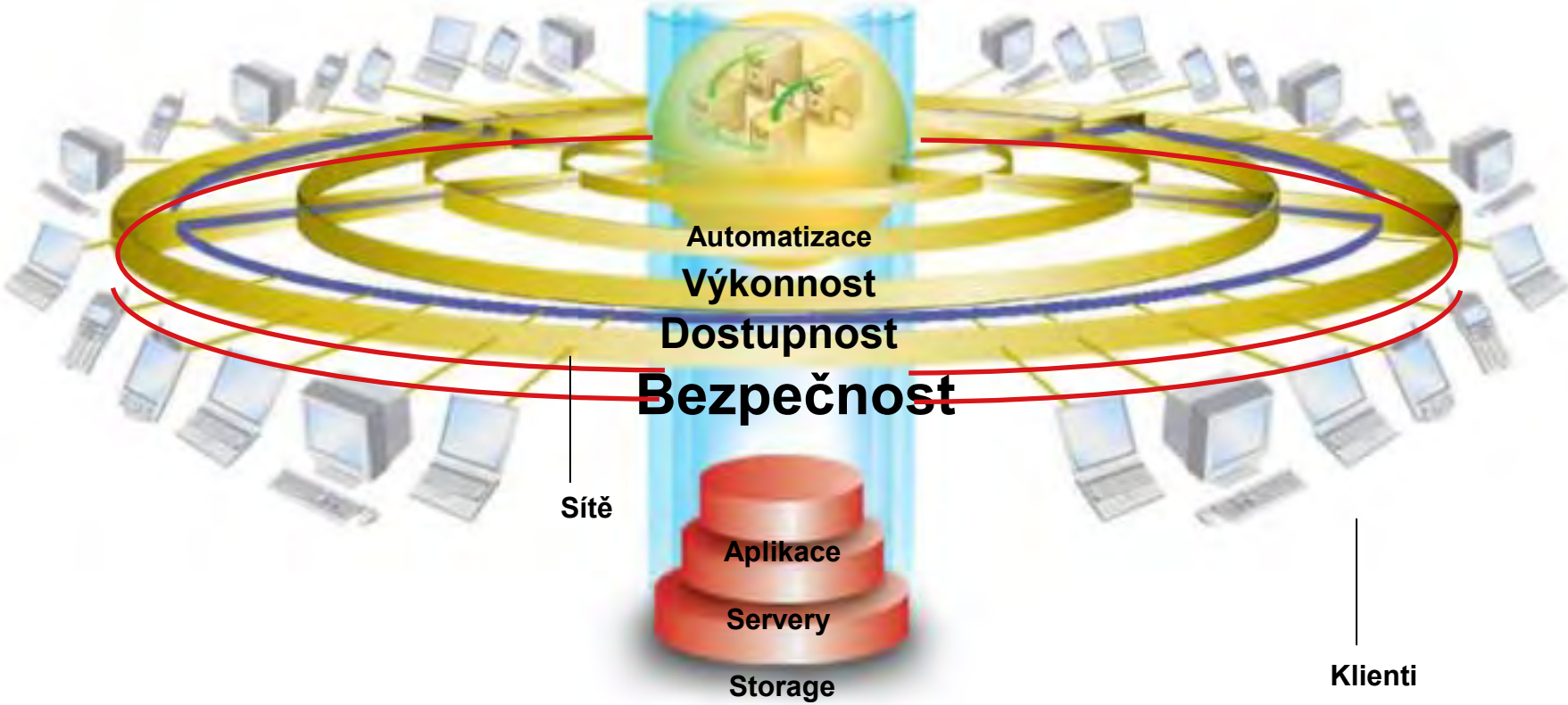
Bezpečnost a provoz – incident nebo epizoda

Složitost – už to všechno máme...

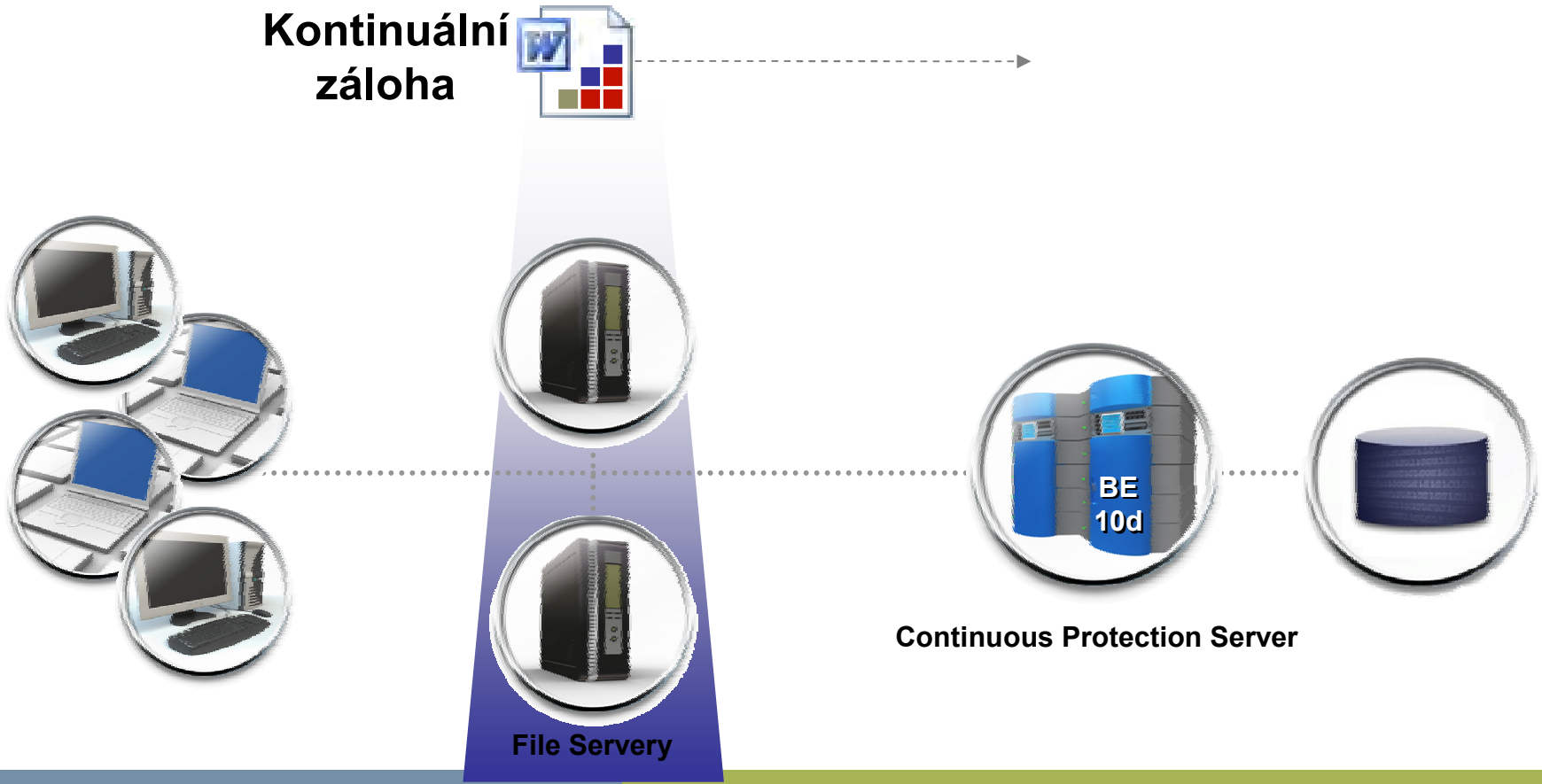
Za méně udělat více!

Udržíme Vás na nohou, v chodu a rostoucí, ať se stane cokoliv !

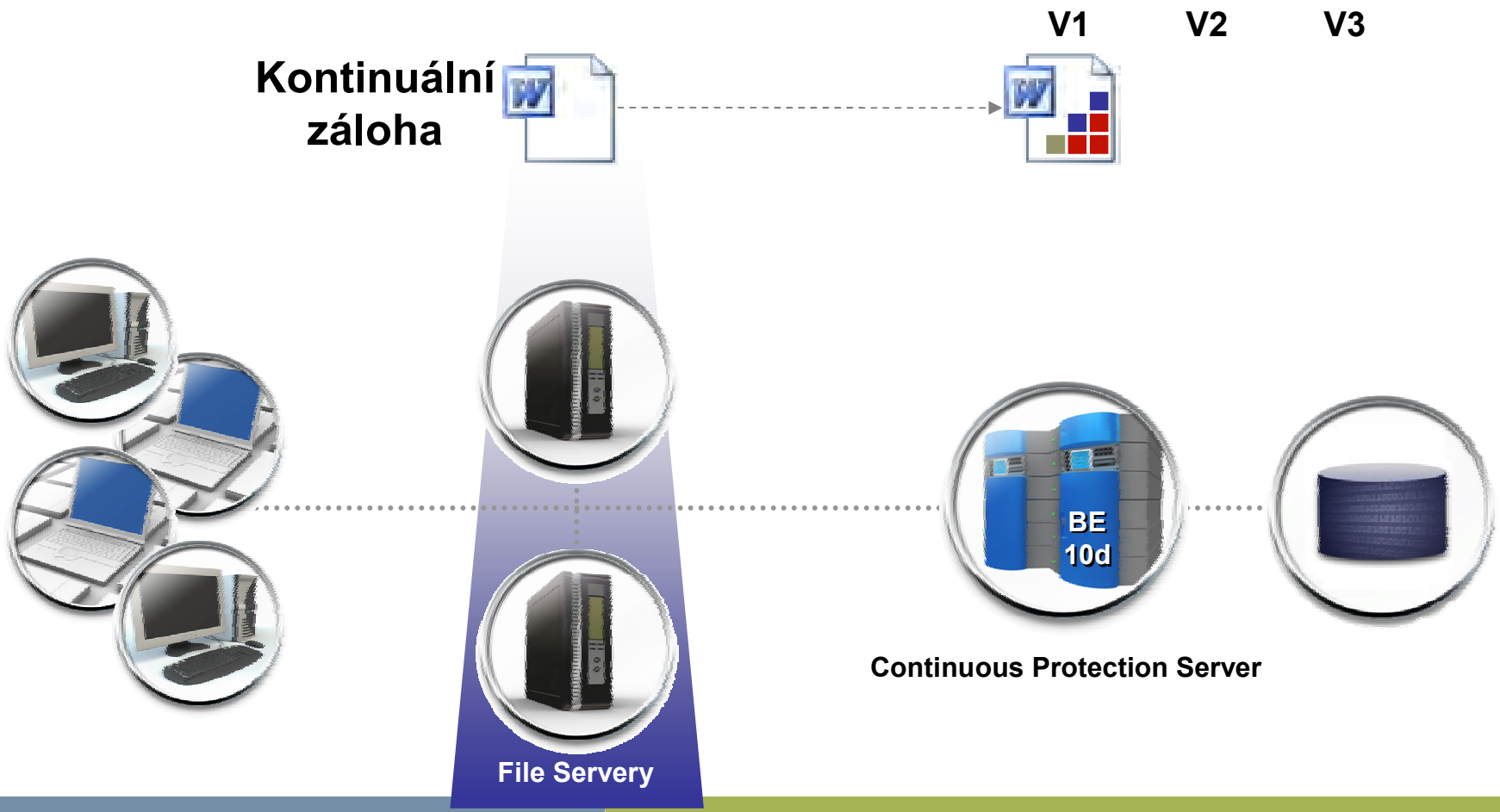
Proaktivní bezpečnost musí konvergovat s dostupností



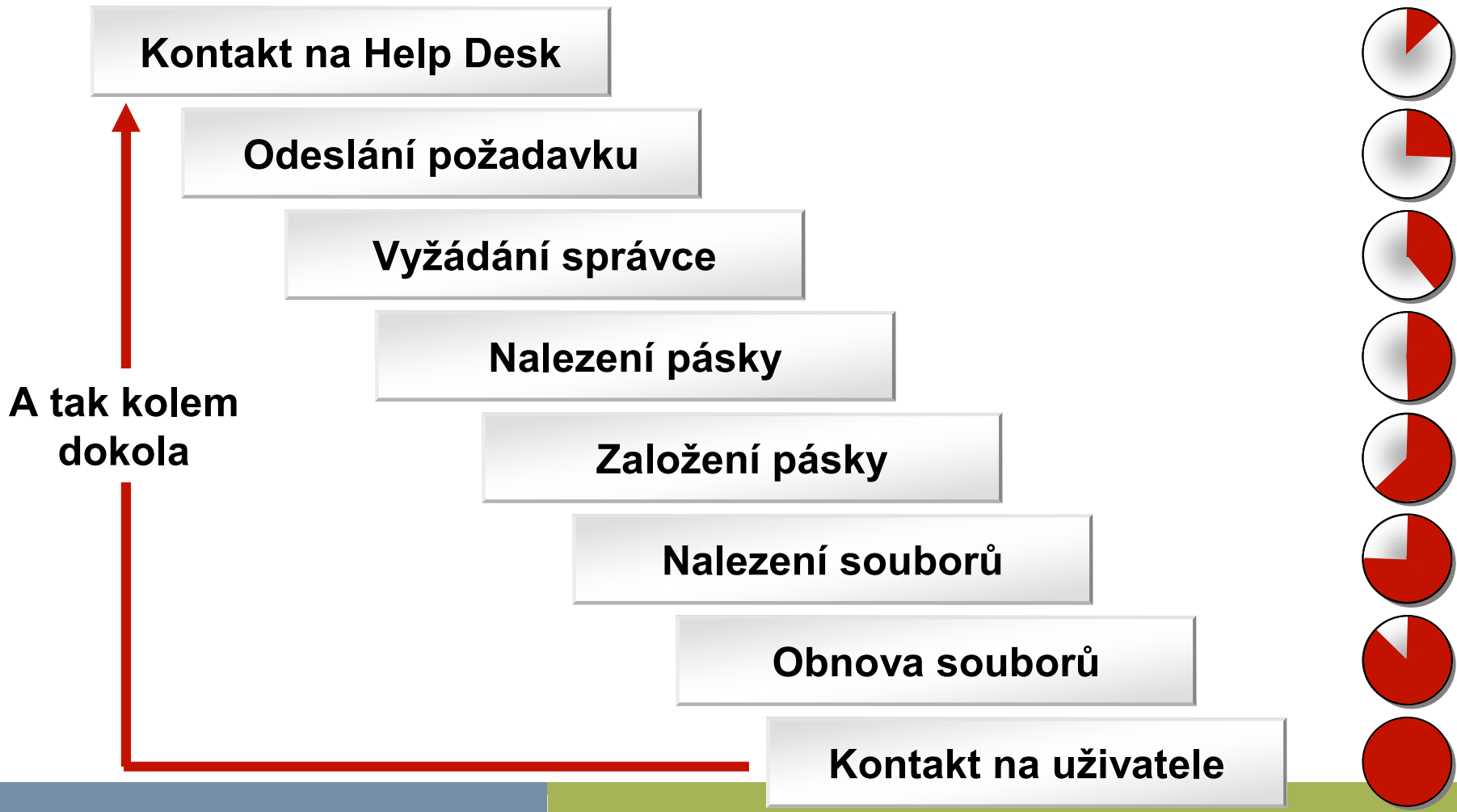
Příklad druhý – kontinuální bezpečnost dat



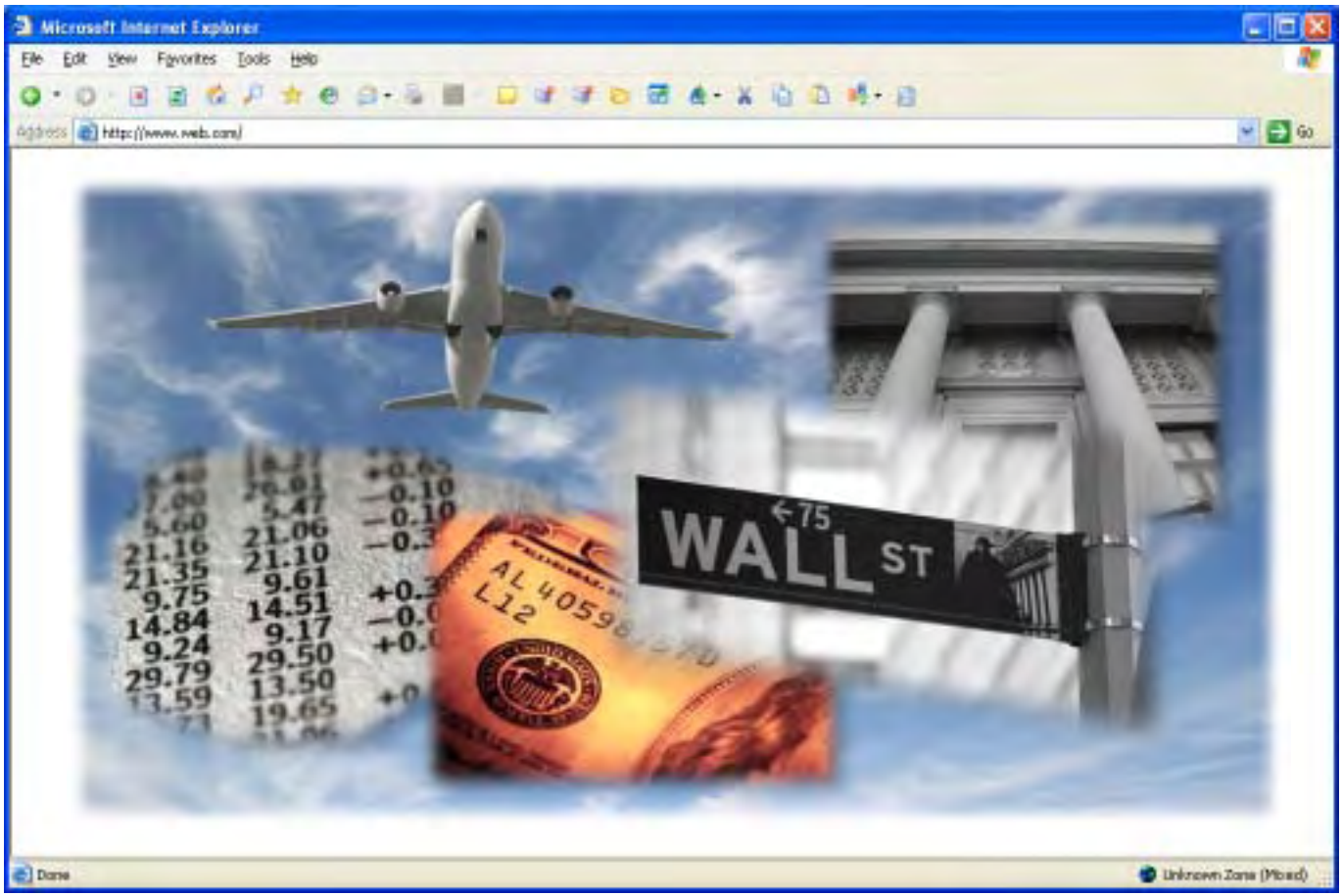
A dokonce ve verzích souborů...



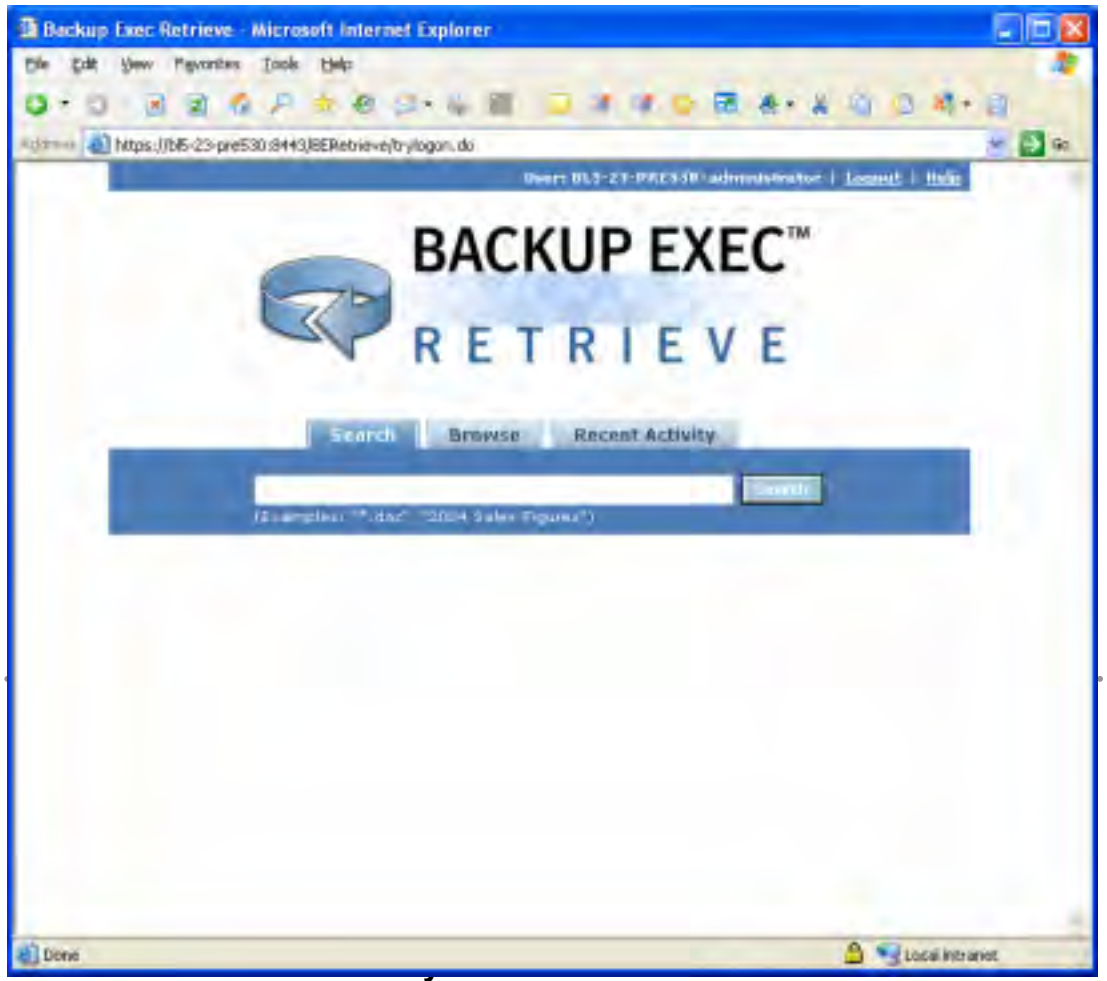
Obnova, jak ji znáte z minula

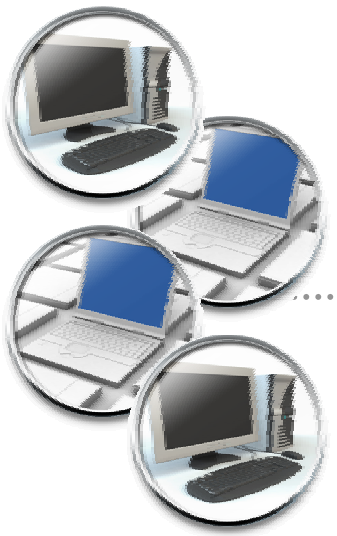


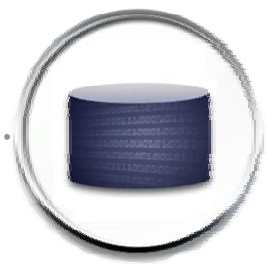
Obnova, jak vypadá dnes



“Google Like” – zvládne každý sám







Příklad třetí – okamžitá obnova systému

Ne	Po	Út	St	Čt	Pá	So
FULL	INCR	INCR	INCR	INCR	INCR	INCR

Plánované & událostmi aktivované body pro Hot System Recovery

Desktopy, notebooky, aplikační servery

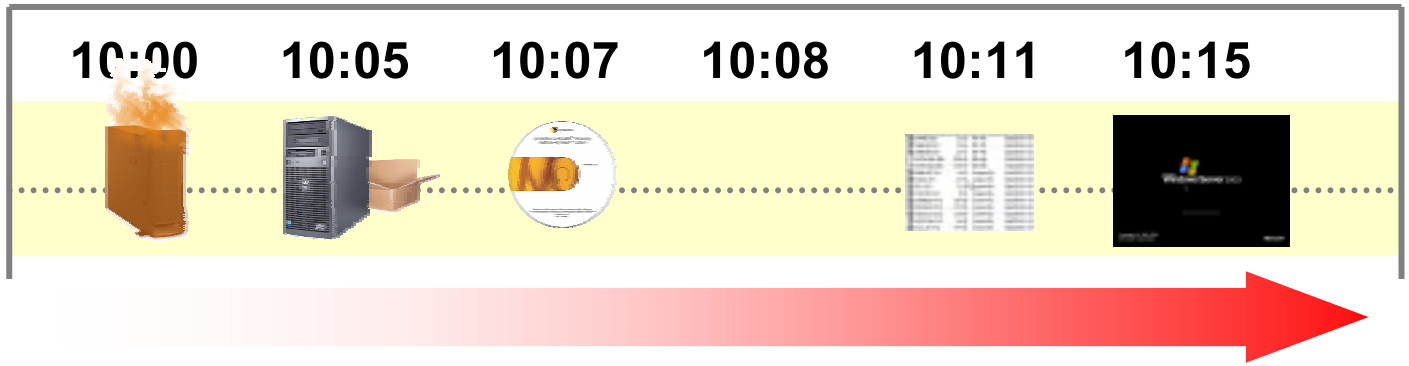
File Servery

Zálohovací server

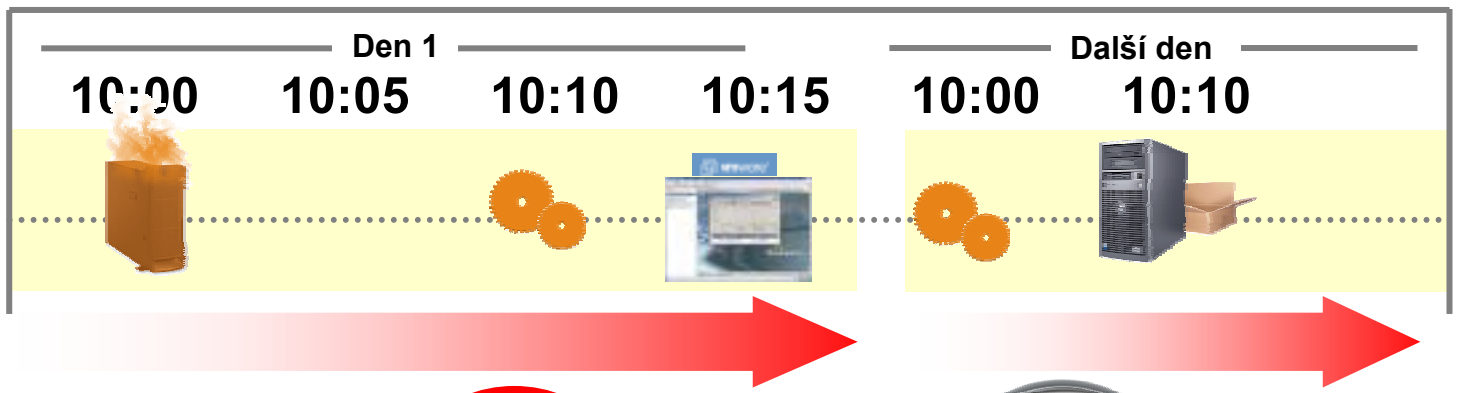
Recovery Manager

Pásková knihovna

Nová cesta: Fyzická obnova (minuty)

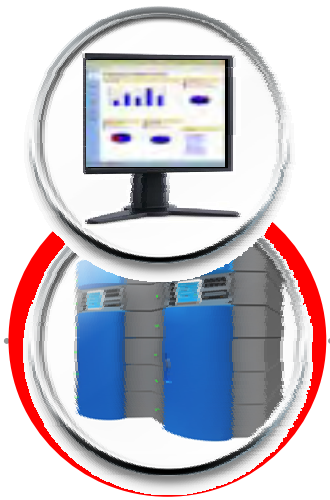


Nová cesta: Virtuální obnova (minuty)



Desktopy, notebooky, aplikační servery

File Servery



Zálohovací server

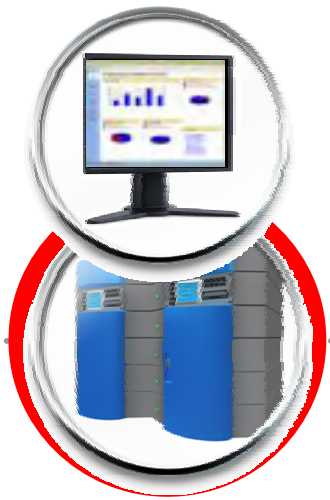
Recovery Manager

Pásková knihovna

Nová cesta: Obnova na dálku (minuty)

Desktopy, notebooky, aplikační servery

File Servery



Zálohovací server

Recovery Manager

Pásková knihovna

Obnova na odlišný hardware

Server 1

- SCSI
- PCI
- Single Processor

Server 2

- SATA
- PCIx
- Dual Processor

DS4BRI.BIT	22 KB	BIT File	8/8/2005 6:55
DSBRI2F.BIT	12 KB	BIT File	8/8/2005 6:55
DSBRI2M.BIT	22 KB	BIT File	8/8/2005 6:55
DSPDLOAD.BIN	808 KB	BIN File	8/8/2005 6:55
DSPDQSIG.BIN	838 KB	BIN File	8/8/2005 6:55
DUBE100.SYS	12 KB	System file	8/8/2005 6:39
DXAPI.SYS	13 KB	System file	8/8/2005 6:55
DXG.SYS	71 KB	System file	8/8/2005 6:55
DXGTHK.SYS	5 KB	System file	8/8/2005 6:55
E100B325.SYS	152 KB	System file	8/8/2005 6:39
E1000325.SYS	172 KB	System file	8/8/2005 6:39
EG1032V2.SYS	135 KB	System file	8/8/2005 6:39
EG103264.SYS	46 KB	System file	8/8/2005 6:39
EL2K_XP.SYS	144 KB	System file	8/8/2005 6:39

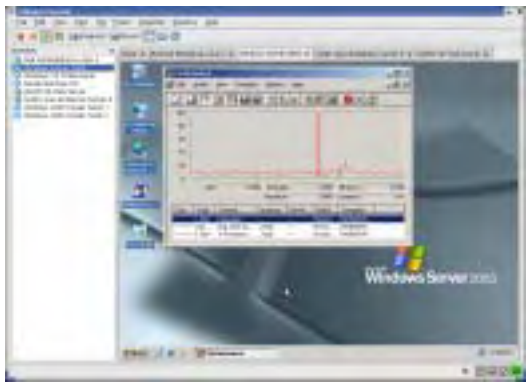
1. Je instalována Restore Anyware Option, je vybrán a uložen bod obnovy.
2. V případwě výpadku může být bod obnovy použit k obnově systému na jiný hardware.
3. Recovery disk obsahuje ovladače potřebné k obnově na zcela jiný hardware. Další lze zavést v průběhu obnovy..
4. Systém je rychle, snadno a spolehlivě obnoven na jiný hardware.

Obnova na „žádný“ hardware

Fyzický systém

Konverzní toolkit

Virtuální systém



1. Restore Anyware Option umožňuje konverzi fyzického systému do virtuálního a zpět.
2. V případě výpadků hardware, pro předinstalační testování nebo migraci systému lze body obnovy konvertovat do virtuálního prostředí
3. Ve virtuálním prostředí může být systém provozován, testován nebo laděn předtím, než je znovu obnoven do fyzického prostředí
4. Zpětná konverze bodů obnovy do fyzického prostředí je rychlá a snadná, jakmile je k dispozici HW.

symantec.

Udržíme Vaše podnikání
v chodu, na nohou a rostoucí,
ať se stane cokoliv !

To je konvergence bezpečnosti a dostupnosti!

Kam se ubírají ostatní a čím k tomu přispějí...?

McAfee

TREND MICRO

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.

INTERNET SECURITY SYSTEMS

Juniper NETWORKS

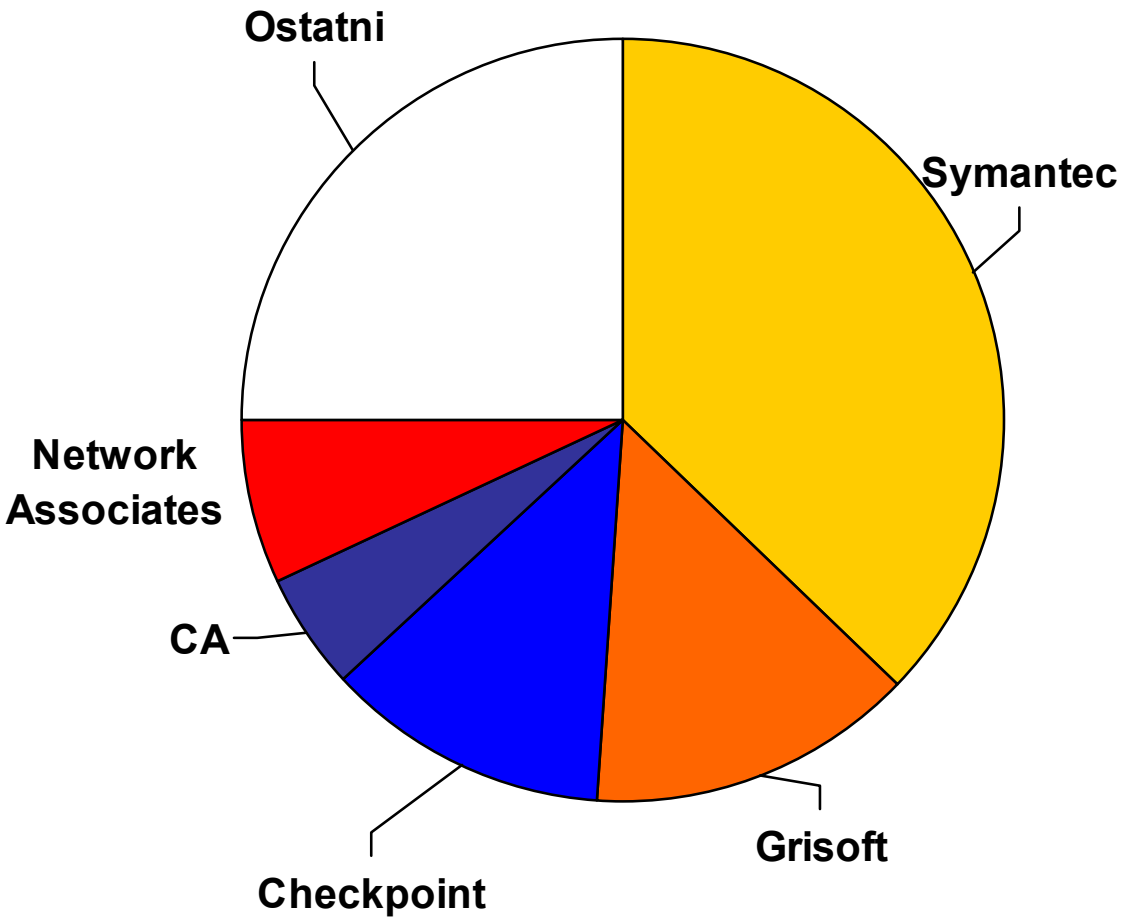
enterasys Networks that Know

Dopady na celé odvětví

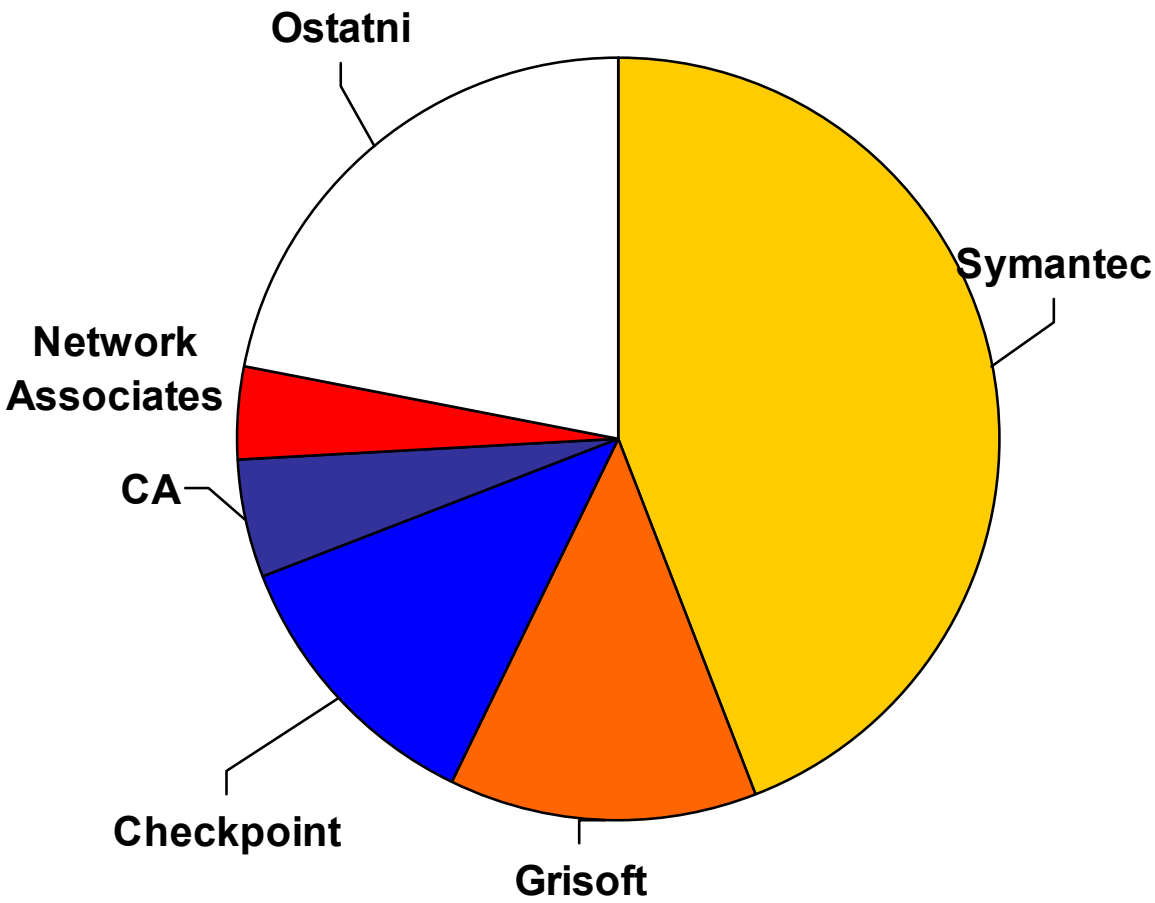
Udržíme Vás na nohou, v chodu a rostoucí, ať se stane cokoliv !

Proč právě Symantec?

Trh bezpečnostního software v ČR - 2004



Trh bezpečnostního software v ČR – odhad 2005

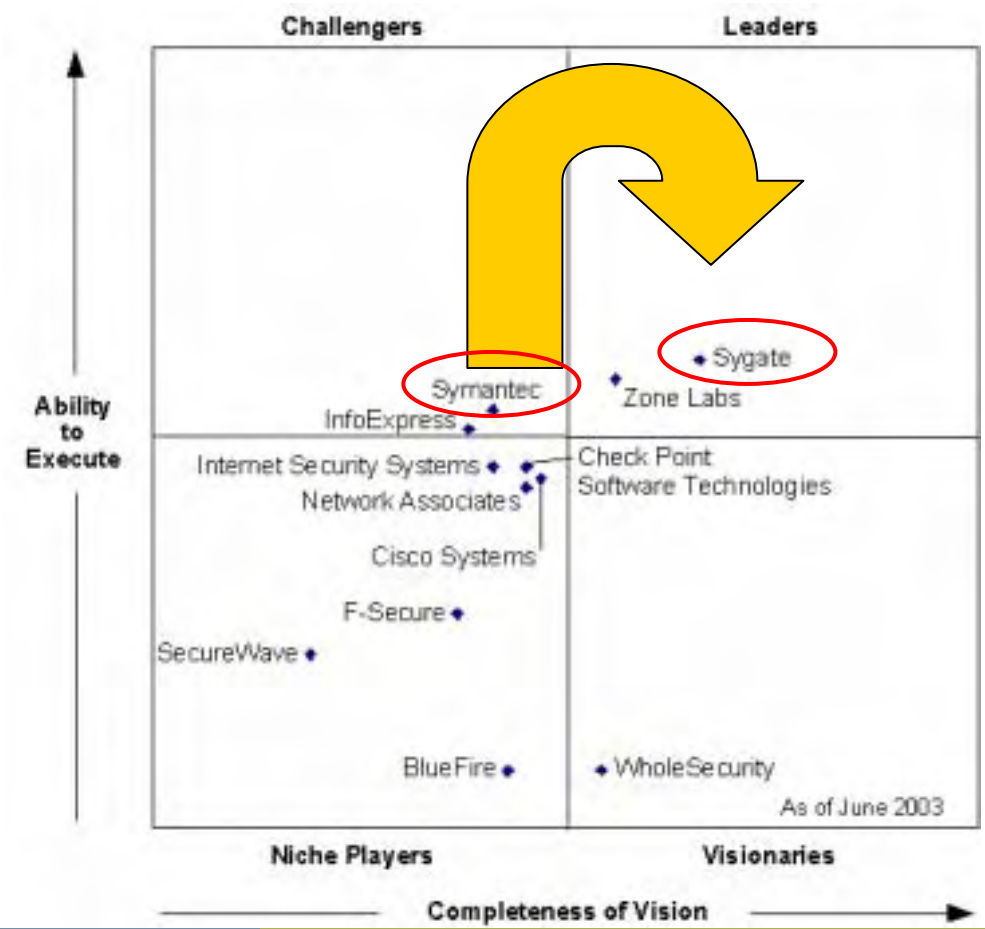


Gartner: Magický kvadrant „Antivirová kontrola“

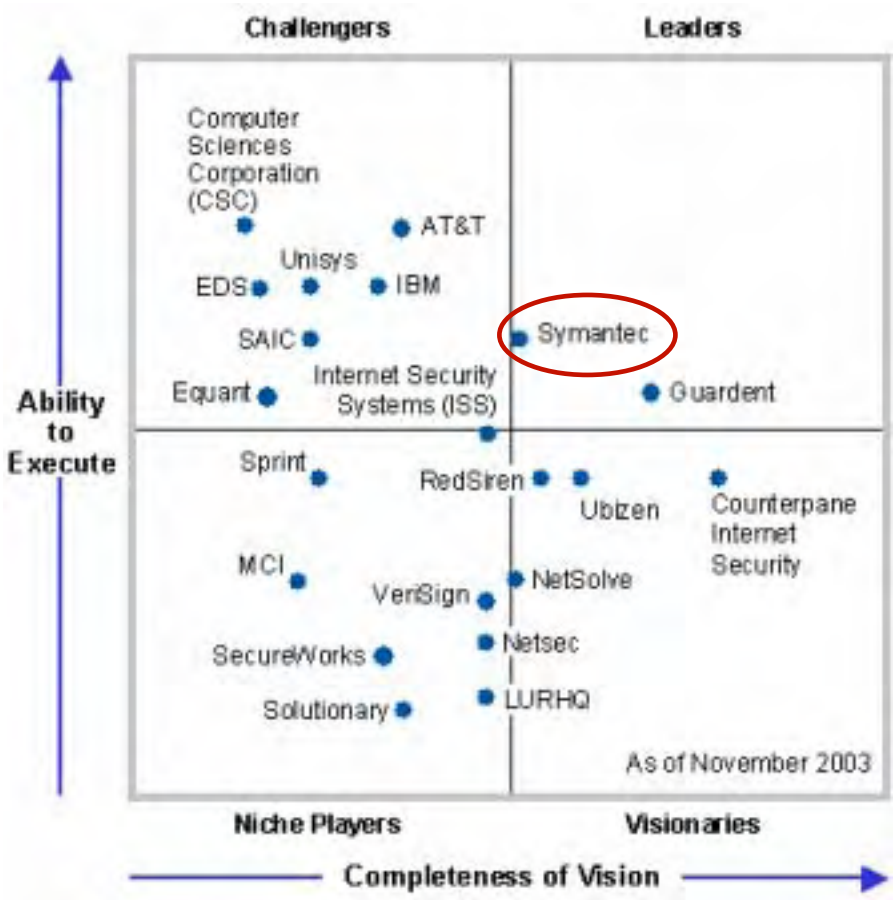
Gartner: Magický kvadrant „Osobní firewally“

V září 2005 Symantec Opět „zaúřadoval“ na bezpečnostním trhu:

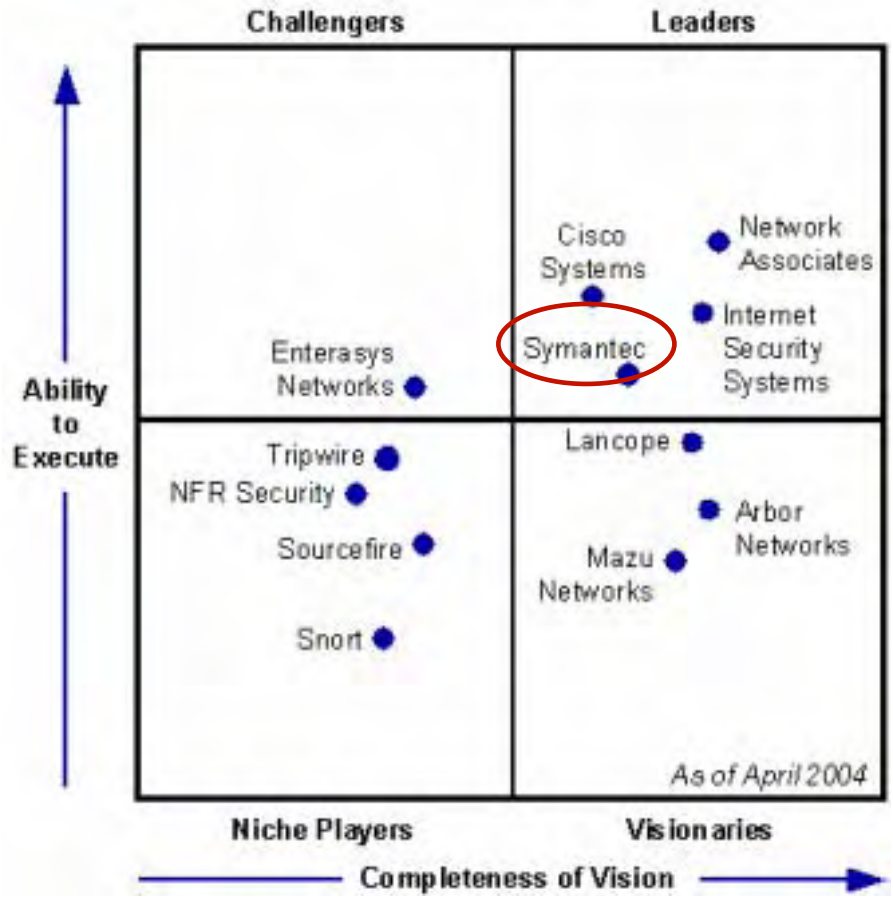
Akvizice společnosti Sygate nám dává první místo v oblasti „End Point Compliance“ a také na trhu s osobními firewally !!!



Gartner: Magický kvadrant „Řízení bezpečnosti“



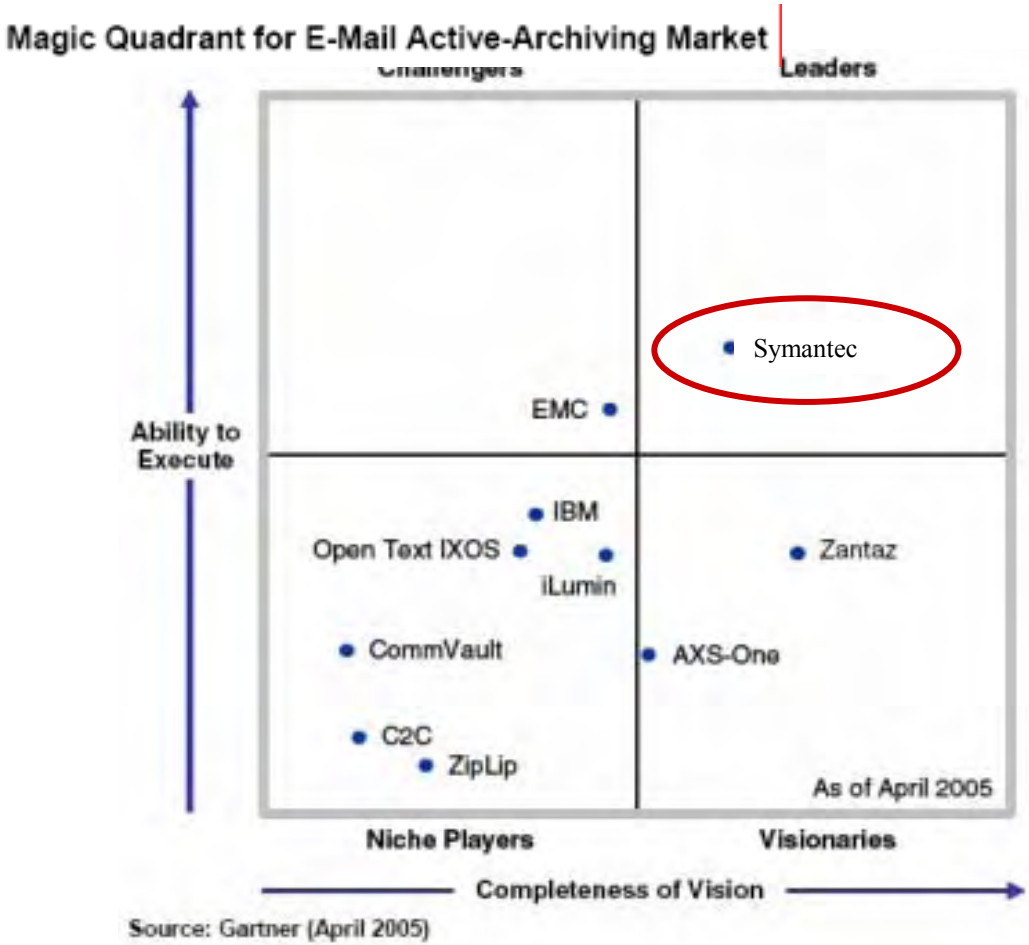
Gartner: Magický kvadrant „Prevence narušení“



Gartner: Magický kvadrant „Bezpečnost pošty“

Gartner: Magický kvadrant „Zálohování a obnova“

Gartner: Magický kvadrant „Aktivní archivace pošty“



Nový ELITE se státní správou na období 2007-2008

- Od prosince 2006 do dubna 2007 bylo již se státními orgány a organizacemi podepsáno přibližně 200 prováděcích smluv
- Úspora vynakládaných prostředků je značná, neboť průměrná nákupní cena dle ELITE smlouvy je o 70% nižší než bežná doporučená na trhu
- Příklady:
  - Ministerstva: financí, práce a sociálních věcí, vnitra, zahraničních věcí, školství, obrany, životního prostředí, pro místní rozvoj...
  - Ústřední orgány: úřad vlády, Nejvyšší kontrolní úřad, Český statistický úřad, Česká obchodní inspekce...
  - Krajské úřady: celkem 12 krajských úřadů a řada městských magistrátů, i menších měst a obcí...

Další příspěvek k Vaší bezpečnosti a dostupnosti

- Po dobu následujících 3 měsíců v jediné licenci „Symantec AntiVirus Enterprise Edition TOTAL PROTECTION“:
  - Kompletní antivirová ochrana
  - Osobní firewally pro dekstopy a notebooky
  - Prevence narušení bezpečnosti počítačů
  - Kompletní antispamová ochrana
- To vše přesně za cenu běžné antivirové ochrany !!!

- Po dobu následujících 6 měsíců snížení ceny software pro dostupnost o 50%
  - Platní pro všechny orgány státní správy a samosprávy

symantec.

Děkuji za pozornost