McAfee
Proven Security™



Myslete jako hackeři

Vladimír Brož, Territory Manager Czech & Slovak Republic

Vladimir_Broz@mcafee.com

Program

- Neznalost neomlouvá. Zaměřeno na hacking.
- Motivace
- Hackingové postupy
- Jak se chránit?

Security Paradox

Vybalancování bezpečnosti a podnikání

Fakta o bezpečnosti

- Velice komplexní vývoj a růst hrozeb
- Méně času na obranu před červy a zero-day úokům
- Hrozby cílí na konkrétní prostředky/aktiva

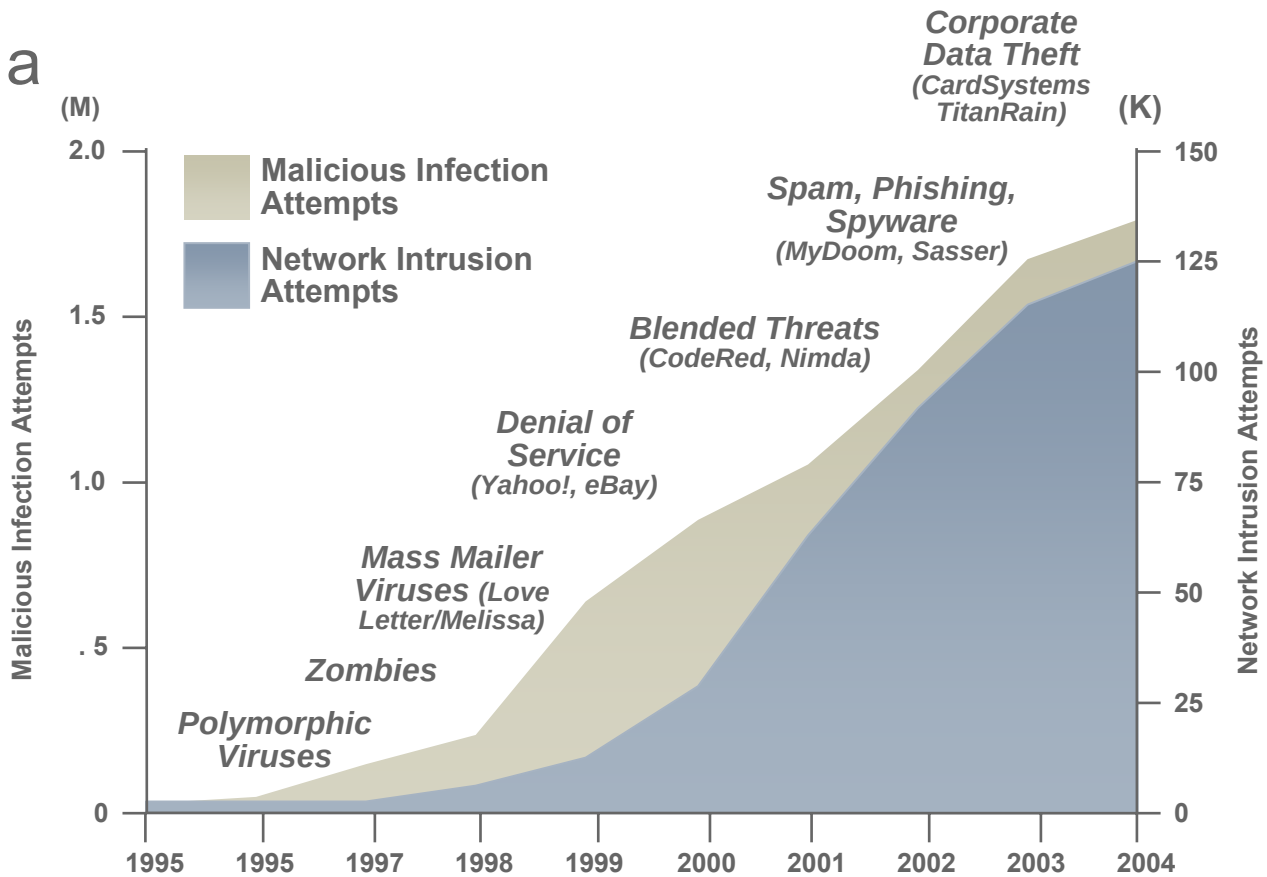


Fakta o podnikání

- Lidská kapacita a omezená bezpečnostní znalost/vědomosti
- Tlak na shodu s regualacemi externími/interními
- Namapování shody a provozu

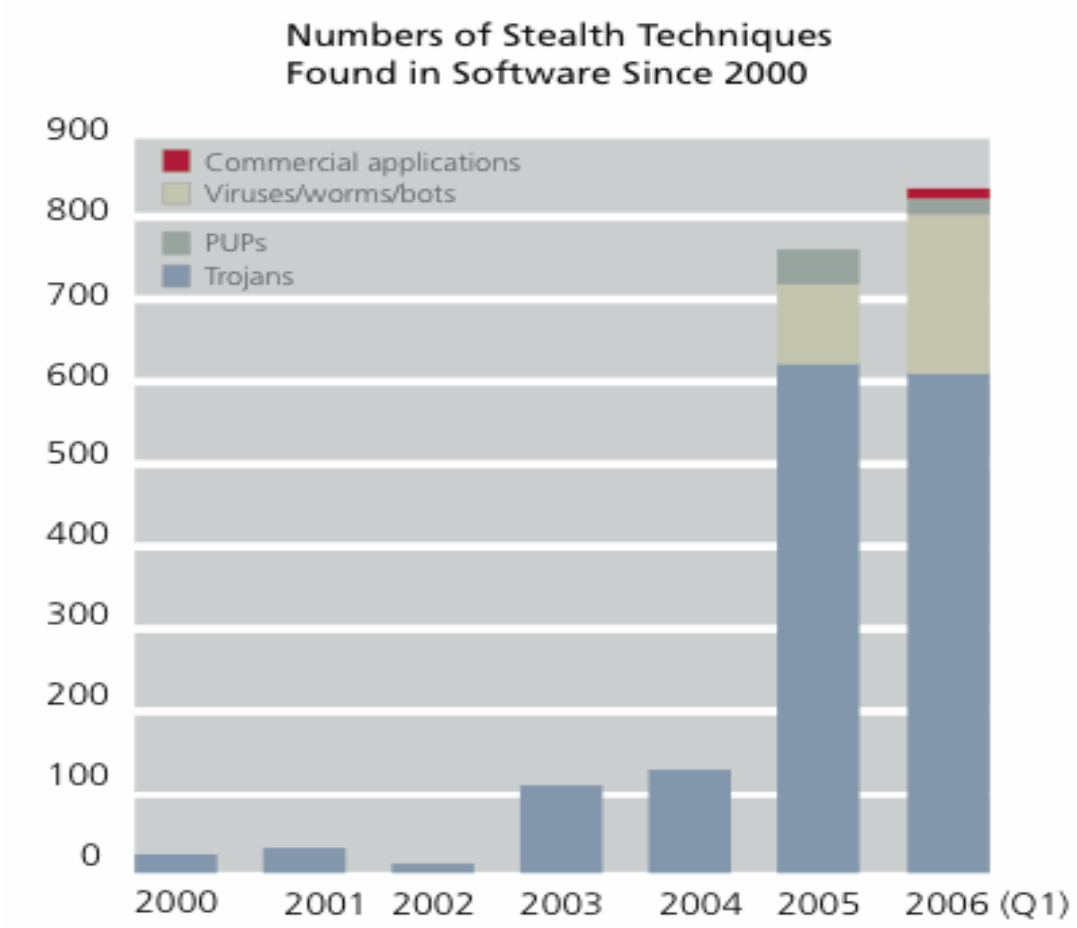
Historie a budocnost útoků

- Zvyšující se počet a komplexnost
- Cíle se mění
  - spotřebitelé
  - podniky
  - národy
- Poslední cíl
  - Krádež dat



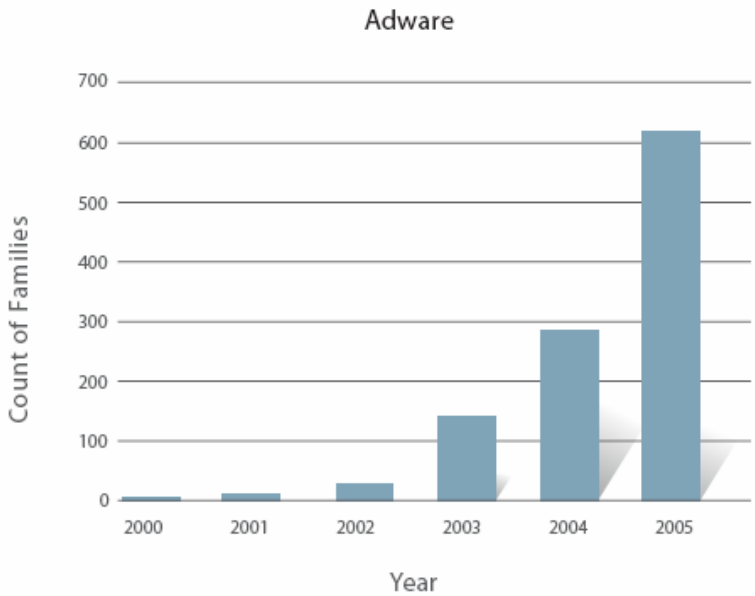
Source: IDC, ICSA, CERT, CSI/FBI, McAfee

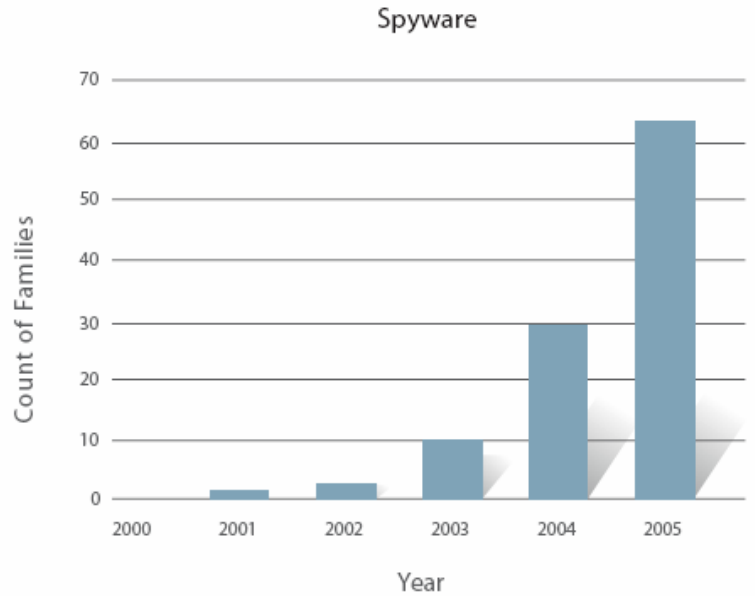
Nárůst rootkitů či „tajných“ technik



Source: McAfee AVERT Labs

Nárůst potencionálně nechtěných programů





McAfee
Proven Security™



Zaměřeno na hacking

Hierarchie „CYBER CRIMINALS“

- Script Kiddies—Obvykle technicky „nevyzrálí“ hackeři používající různé nástroje“. Neuvědomují si plně důsledky ilegálního jednání
- Cyber Punks—Více vzdělaní útočníci, kteří se zaměřují na „zohyzdění“ webovských stránek obětí nebo další poškozující aktivity
- Hackers/Crackers—Obvykle někdo kdo doopravdy rozumí technologi, kterou používá a někdo kdo má jasnou představu o cíli a záměru své ilegalní aktivity.
- Cyber Gangs—Skupina hackerů zformovaná k nové vlně organizovaného zločinu.

Existují dva 2 typy hackingových útoků:

- Příležitostné
  - Míří na miliony PC
  - Mají malou úspěšnost, ale velký počet obětí v absolutních číslech.
  - Často se zaměřují na lidské slabosti:
    - Nigerijské scamy
    - Vtipy/ šetřiče obrazovky.
- Cílené
  - Zaměřují se na jednotlivce nebo vybrané společnosti
  - Cílené útoky následují po příležitostných útocích, ze kterých získávají data.
  - Zkušené hackery charakterizuje trpělivost a pečlivé plánování.

Neznalost neomlouvá

- Nezkušené a nevědomé oběti jsou bezbranné
- Hackingové postupy jsou často použity při cílených útocích
- Jen poučené oběti se mohou chránit či minimalizovat škody

Příležitostný hacking

- Ze svých vlastních PC spouštějí útoky jen amatéři a jedinci v „bezpečných“ zemích.
- Je možné si pronajmout armády Zombie. Ty hackerům umožňují útočit na miliony PC na internetu, aby rozesílaly spam a na dálku spouštěly zero-day exploity.
- Hackeři mohou:
  - Vybudovat svoji vlastní zombie armádu pro budoucí zero-day útoky nebo Distributed Denial of Service útoky (DDoS).
  - Instalovat keyloggery.
  - Krást hesla.
  - Krást informace z prohlížeče uložené v paměti: jména uživatelů, hesla, čísla kreditních karet, účty na webu.
  - Automaticky zkoušet tato uživatelská jména/hesla na ebay, paypal, hotmail, natwest nebo jiných serverech.

Příležitostný hacking (pokračování)

- Útoky hrubou silou:
  - Zaměřuje se na e-Bay, Yahoo, Hotmail s automaticky generovanými jmény a s 50 nejpoužívanějšími hesly nebo používá http://geodsoft.com/howto/password/common.htm.
  - To umožní přístup k několika stovkám účtů, které mohou být zneužity pro sociální inženýrství, finanční a citlivé materiály. Jinak může být použit pro šíření spamu nebo malwaru.

- Další příležitostný hacking
  - Wardriving (hacking bezdrátových sítí): má auto, anténu, cestuje.
    - Více než 50 % uživatelských přístupových bodů (Wireless Access Points) nepoužívá šifrování.
    - Více než 90 % těch, které mají WEP používá 40bitové šifrování.
  - Dumpster diving (prohledávání odpadků):
  - Použitý hardware: většina diskových mechanik nebyla účinně smazána. Tajné informace mohou být snadno obnoveny s použitím speciálních programů: často se podaří obnovit tajná či finanční data.

Příležitostný hacking (pokračování)

- Informace sesbírané při náhodném hackingu jsou často použity jako základ pro cílený hacking.
- Vyšší dostupnost osobních dat:
  - Google. Nástroj používaný více než 95 % hackerů pro získávání dat.
  - MySpace.com, bebo.com, Yahoo 360. Velké rozšíření osobních dat. Časté informace o tom, kde osoba žije, jaké má přátele, kde tráví svůj čas, koníčky.
  - Blogging: pochopení cílů, obav, názorů a psychiky blogera.
  - LinkedIn.com, OpenBC: prohlednutí životopisu cíle. Kde pracují, kdo jsou jejich kolegové
  - Tato místa jsou vynikajícím zdrojem informací pro hackery, kteří data zneužívají k provádění sociálního inženýrství. Hackeři se tak mohou vydávat za blízké přátele/kolegy/příbuzné a získat citlivé informace.

Cílený hacking - jednotlivci

- Často je prováděn důvěryhodnými osobami.
  - Podezíraví partneři
  - Zaměstnanci
- Keylogging
  - Je používán velmi často. Ale vyžaduje fyzický nebo vzdálený přístup k počítači.
  - Mnoho spywarových programů a malwaru obsahuje keyloggery.
  - Často jsou získány osobní e-maily, finanční účty a hesla.

Cílený hacking – jednotlivci(pokračování)

- Cílové osoby jsou často nalezeny technikou „odrazového můstku“ (springboarding)
  - Cíl1 už byl kompromitován. Získaná hesla už má k dispozici hacker.
  - Hacker tyto informace použije, aby zjistil povahu a rozsah vztahu mezi Cílemt1 a potenciálními cíli.
  - Hacker použije sociální inženýrství k získání informací, které kompromitují Cíl2.
  - Cíl2 je úspěšně využit a poslouží jako odrazový můstek pro další lukrativní cíl.
- Získává zprávy o úvěrech/půjčkách a klíčová osobní data o cílech. Může být použit pro získání kreditních karet, půjček.
- Osobní vydírání. Prohledávání e-mailů může zviditelnit minulé neuváženosti, které chce cíl udržet v tajnosti.
- Mnoho jednotlivců se neobrátí na úřady kvůli těžkostem.

Cílený hacking – společnosti

- Jestliže jde o útok z vnějšku, bude pravděpodobně postupovat podle hackingové metodologie
- Jestliže je riziko odhalení malé, může se pokusit o příležitostný (oportunistický) hacking.
  - Dumpster diving
  - Může předstírat, že má na místě skutečně co dělat. Může nainstalovat Wireless Access Point nebo odposlouchávání hesel.
  - Může na místě zanechat malware (např. USB klíčenky s automaticky spouštěným keyloggerem).
  - Pokusit se o sociální inženýrství k získání důležitých informací nebo přístupu. Může využít informace ukradené při příležitostném hackingu. Může kontaktovat bývalé zaměstnance a předstírat, že je headhunter.

Finanční stimuly

- Schopnost prodávat a obchodovat s funkčními bankovními účty, informacemi o kreditních kartách a osobními ID na IRC kanálech.
- ‘Stipendia’ udělovaná organizovaným zločinem za odhalení zranitelností a exploit kódů. Ty jsou pak použity pro cílené útoky: Nedávný německý exploit Wordu.
- Vydírání:
  - Osobní vydírání může být následkem keyloggingu, přečtení e-mailu nebo odhalení indiskrétností
  - Kvůli nákladům a poškození značky, které může být následkem veřejného zneužití společností, mohou být vedoucí pracovníci v pokušení zaplatit vyděrači ‘úplatek za mlčení’.
  - Korporátní vydírání velkého rozsahu, finanční transakční servery s vysokou marží (např. online kasina). Běžně jsou používány 0-day exploity a DDoS útoky.
- Nákupy zboží:
  - Použití ukradených informací o kreditních kartách a zkompromitované účty
  - Zboží je doručeno nic netušícím třetím stranám, které obdrží nominální poplatek za odeslání zboží do ciziny.
  - Technické zboží se používá pro vybudování účinnějších „virových dílen“. Některé mají oddělení QA a provádějí rozsáhlé testování.
  - Zboží je přeprodáno do ciziny a konvertováno na hotovost.

Finanční stimuly (pokračování)

- Převody hotovosti:
  - Z bankovních účtů a PayPal.
  - Na bankovní účty nic netušících majitelů – tyto účty slouží jako prostřednící pro praní špinavých peněz.
- Krádeže identit
  - Na jméno osoby získají půjčky, hypotéky a kreditní karty.
  - Krádeže laptopů VA, ztráta laptopů E&Y
  - Identity mohou být prodávány na otevřeném trhu.
- Rychlá evoluce s cílem peněžních zisků. Jsou vytvářena nová „odvětví“ pro prodej kradeného zboží a informací.

McAfee
Proven Security™



Postupy hackerů

Postupy hackerů

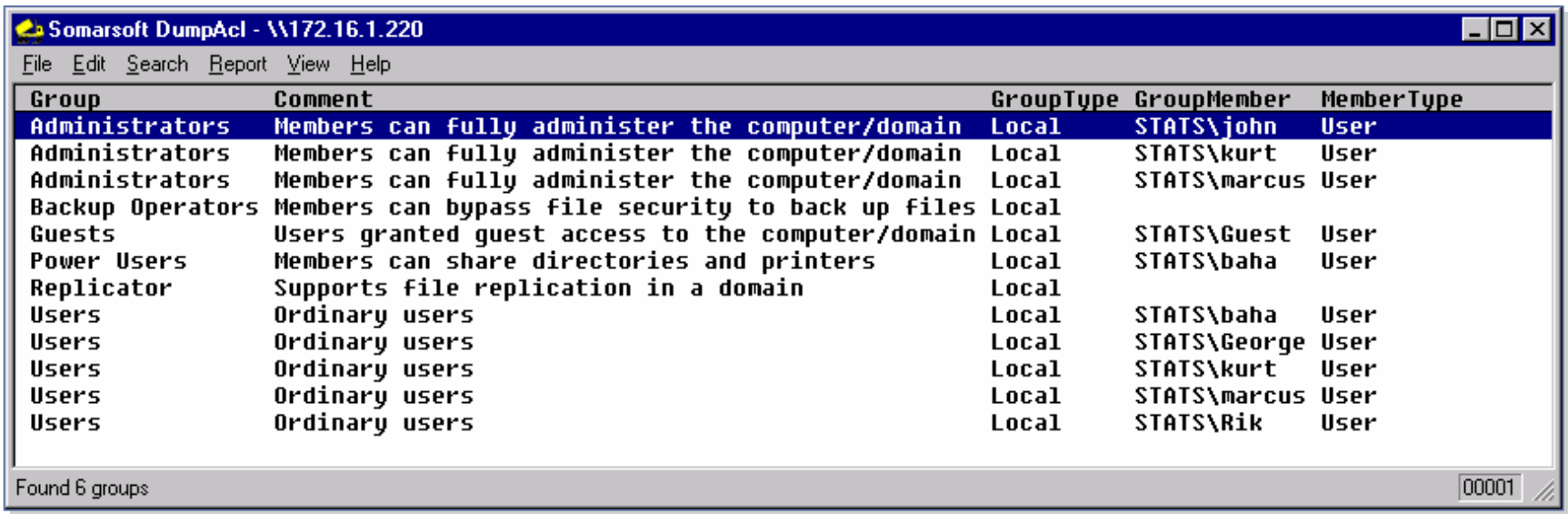
▶ Otisk	Porozumění prostředí
▶ Skenování	Nalezení hosts/services
▶ Zjišťování	Nalezení zranitelných/slabých obětí
▶ Vniknutí	Útok na oběť
▶ Stupňování	Stát se administrátorem/rootem
▶ Loupení	Utajení prvního útoku/získání info
▶ Interaktivita	Začátek remote control/skrytý kanál
▶ Rozšíření vlivu	Získání dalších dat/útok
▶ Úklid	Zajištění zametení stop

Postupy hackerů

- Otisk
- Skenování
- **Zjišťováni**
- Vniknutí
- Stupňování
- Loupení
- Interaktivita
- Rozšíření vlivu
- Úklid

Zjišťování ve Windows, Unix

- Zjišťování charakteru sítě
  - Zjisti, jak jsou systémy propojeny jeden s druhým
- Zjišťování informací o hostitelském systému
  - Najdi informace, které jsou volně dostupné



Group	Comment	GroupType	GroupMember	MemberType
Administrators	Members can fully administer the computer/domain	Local	STATS\john	User
Administrators	Members can fully administer the computer/domain	Local	STATS\kurt	User
Administrators	Members can fully administer the computer/domain	Local	STATS\marcus	User
Backup Operators	Members can bypass file security to back up files	Local		
Guests	Users granted guest access to the computer/domain	Local	STATS\Guest	User
Power Users	Members can share directories and printers	Local	STATS\baha	User
Replicator	Supports file replication in a domain	Local		
Users	Ordinary users	Local	STATS\baha	User
Users	Ordinary users	Local	STATS\George	User
Users	Ordinary users	Local	STATS\kurt	User
Users	Ordinary users	Local	STATS\marcus	User
Users	Ordinary users	Local	STATS\Rik	User

Postupy hackerů

- Otisk
- Skenování
- Zjišťování
- Vniknutí
- Stupňování
- Kořistění
- Interaktivita
- **Rozšíření vlivu**
- Úklid

Co je za rootem

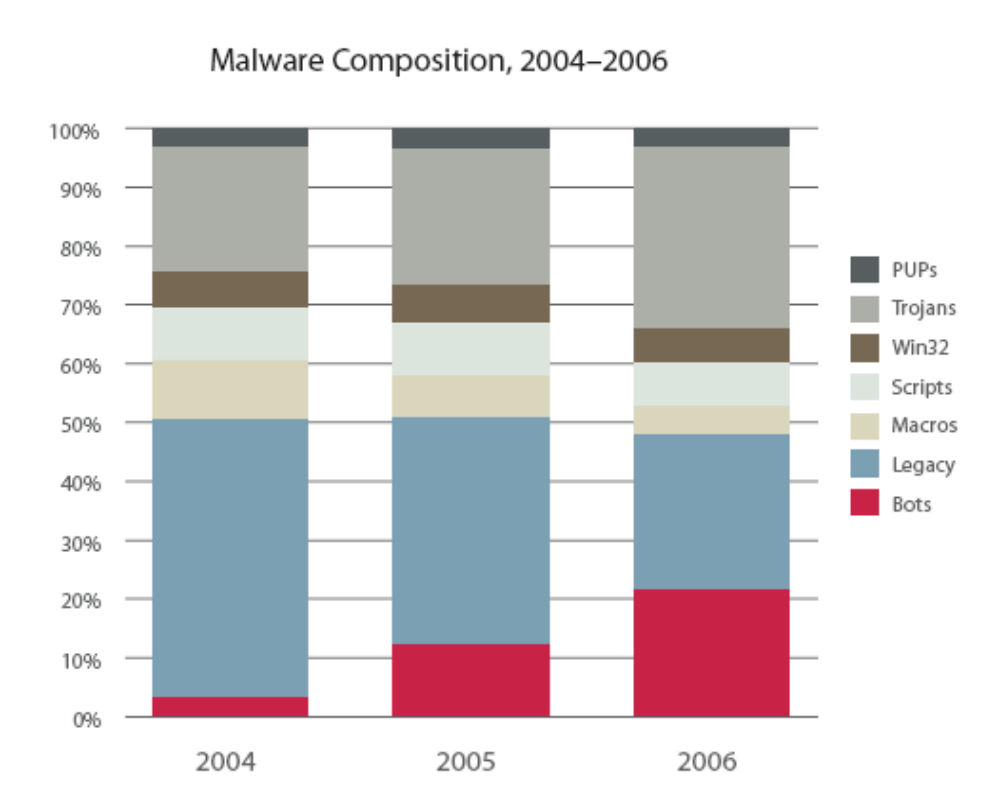
- Použij zkompromitovaný systém pro získání informací
- Použij zkompromitovaný systém jako výchozí bod pro další útoky
- Skryj svůj přístup
- Urči, jak zkontrolovat, jestli byl systém zkompromitován

McAfee
Proven Security™

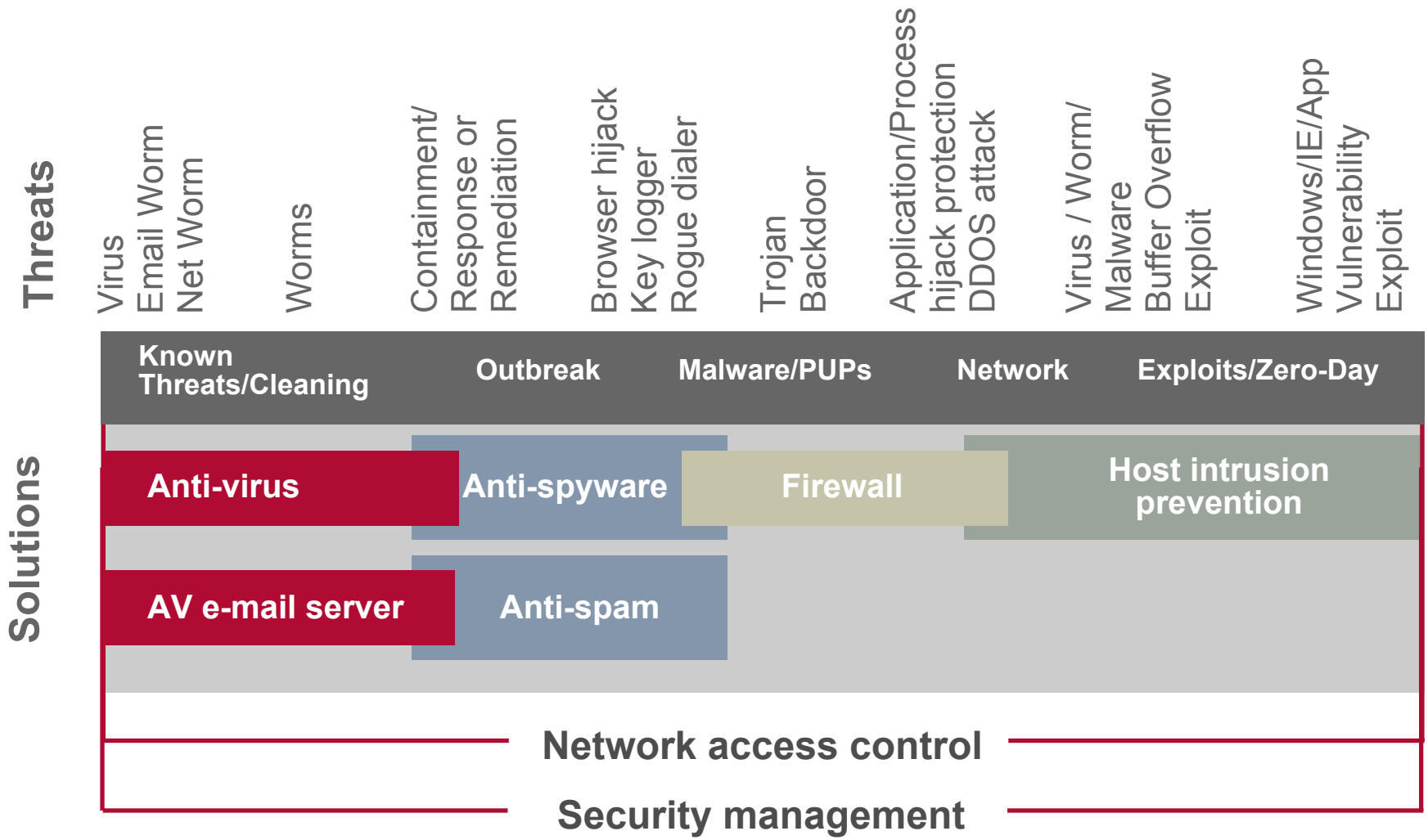


Jak se může bránit?

Jak to nyní vypadá s malware



Komplexní a vyvíjející se hrozby vyžadují bezkompromisní ochranu



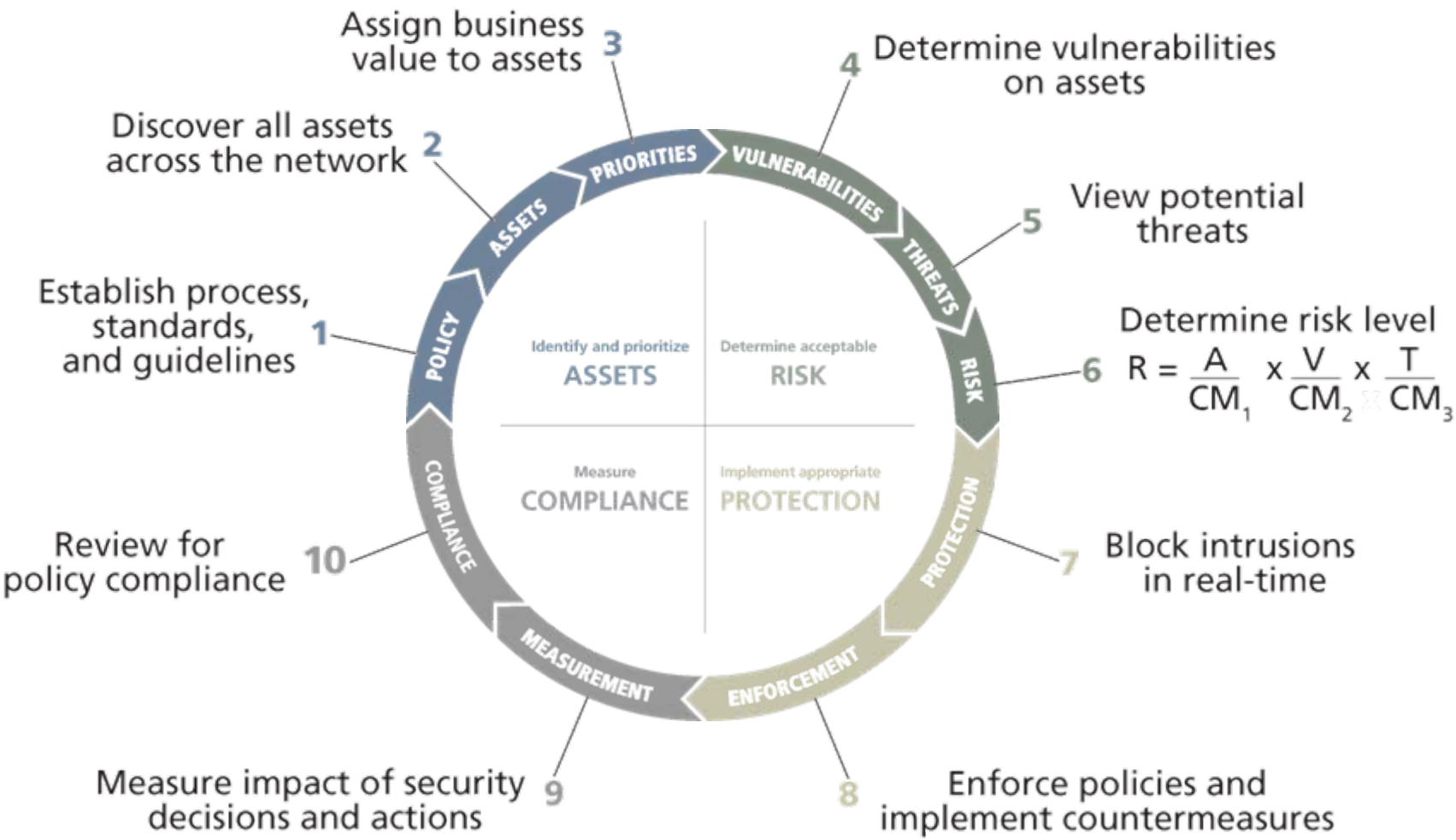
Vícevrstvá ochrana

- Antivir už nestačí:
  - E-mail mohou odkazovat na phishingové weby
  - Počítače se mohou stát DDoS Zombie. 0-day útoky mohou vyžadovat ochranu před nežádoucím vniknutím - **Host Intrusion Protection.** Na počítače běžných uživatelů je velice často instalován spyware
    - Krádeže dat
    - Zpomaluje počítače
- Síťový firewall už nestačí:
  - Bezdrátové sítě vyžadují ochranu. Bezpečnost musí být zapnutá. Statické WEP klíče nestačí

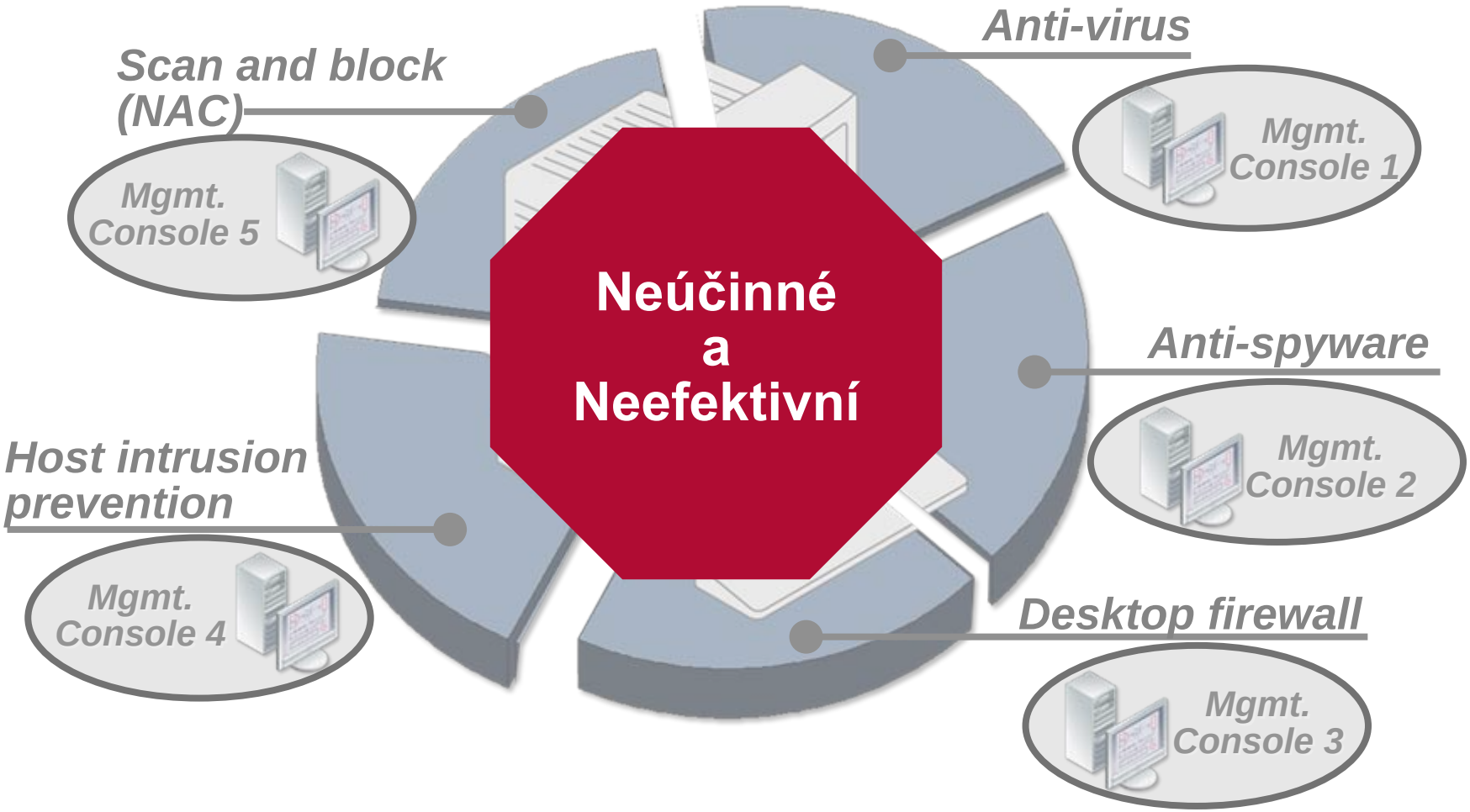
Vícevrstvá ochrana

- Co je třeba?
  - Vícevrstvá ochrana
    - Desktop
      - + Antivir
      - + Anti-Spyware
      - + Desktop Firewall nebo Host Intrusion Prevention
      - + Antispam
      - + Je bezpečný server?
    - Síť
      - + Bezpečné Wireless Access Points
  - Dvě možnosti:
    - Integrovaná řešení versus neintegrovaná řešení

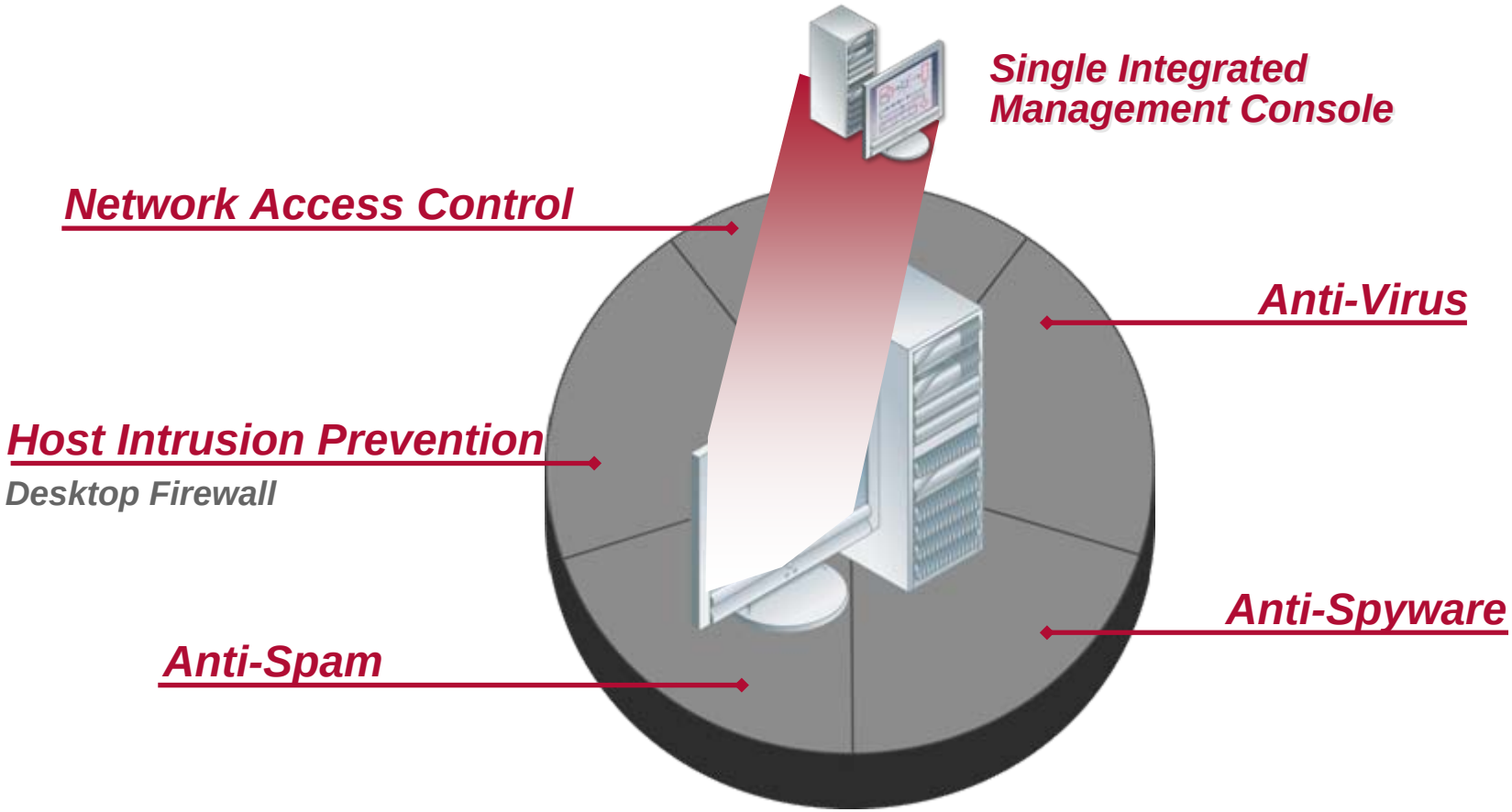
McAfee Security Risk Management Model



Produktový přístup k systémové bezpečnosti

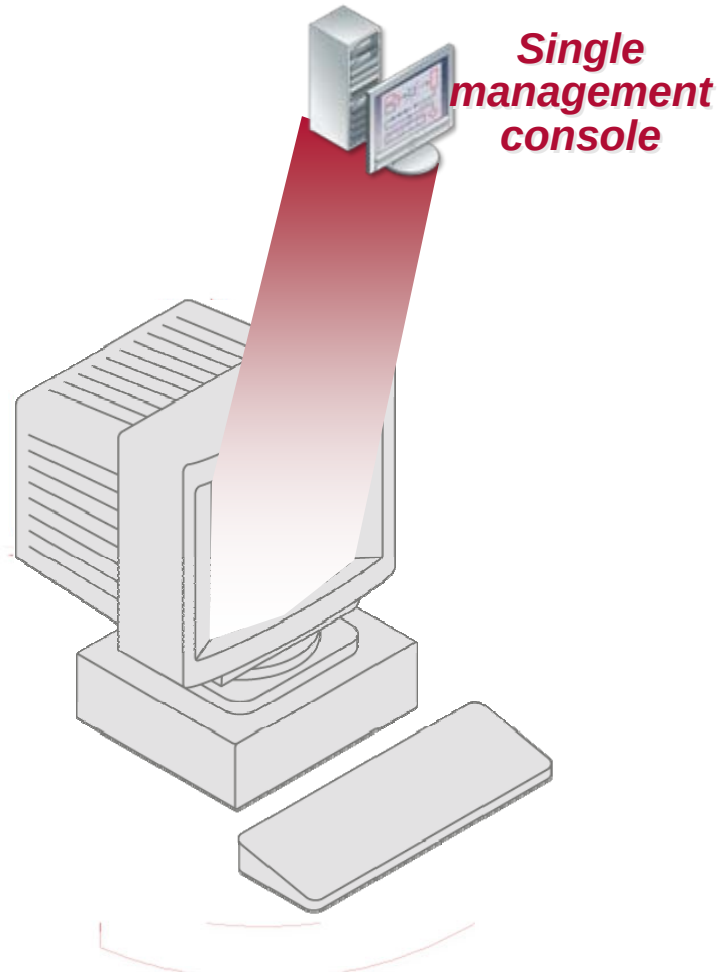


McAfee přístup k integrované systémové bezpečnosti



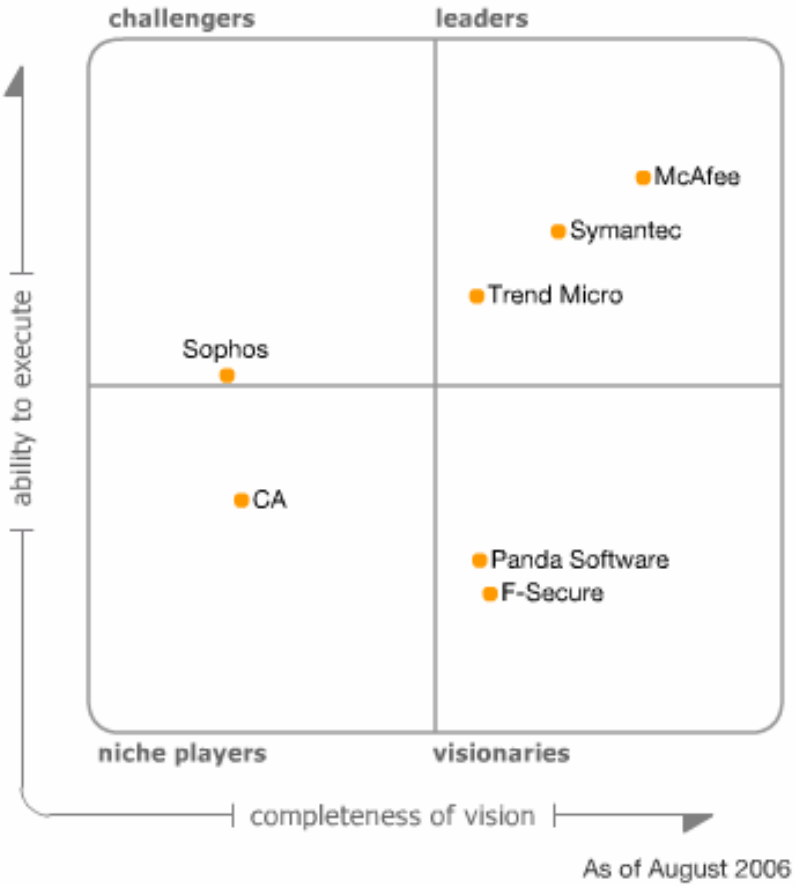
Přínos integrované bezpečnosti

- Identifikace a utěsnění mezer ve vaší ochraně koncových bodů
- Redukce výpadků způsobených infikovanými nebo mimo shodu připojenými koncovými body do sítě
- Redukce času potřebného na reakci proti hrozbě, efektivnost
- Umožní propojení s širšími procesy shody a risk managementu
- Podpora existujících investic do infrastruktury



No Compromise – Anti-Virus

Gartner Magic Quadrant for Enterprise Antivirus 2006, Arabella Hallawell and Peter Christy



This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from McAfee, Inc.



Děkuji za pozornost

Vladimir_Broz@mcafee.com