# CA Integrated Threat Management


- Michal Opatřil
- Consultant
- michal.opatril@ca.com

# Bezpečnostní hrozby

**Cílem IT služeb je zajistit chod business procesů**

- Obrana proti bezpečnostním útokům
- Ochrana nejenom před viry
- Další hrozby spyware, spam, keyloogers, rootkits, malware

# Typy útoků

- Už nemluvíme o jednom viru, jediném napadení
- Na stanicích nalézáme malware, viry dohromady
- Často vidíme více virů na stanicích
- Nelze již používat jeden engine pro kontrolu

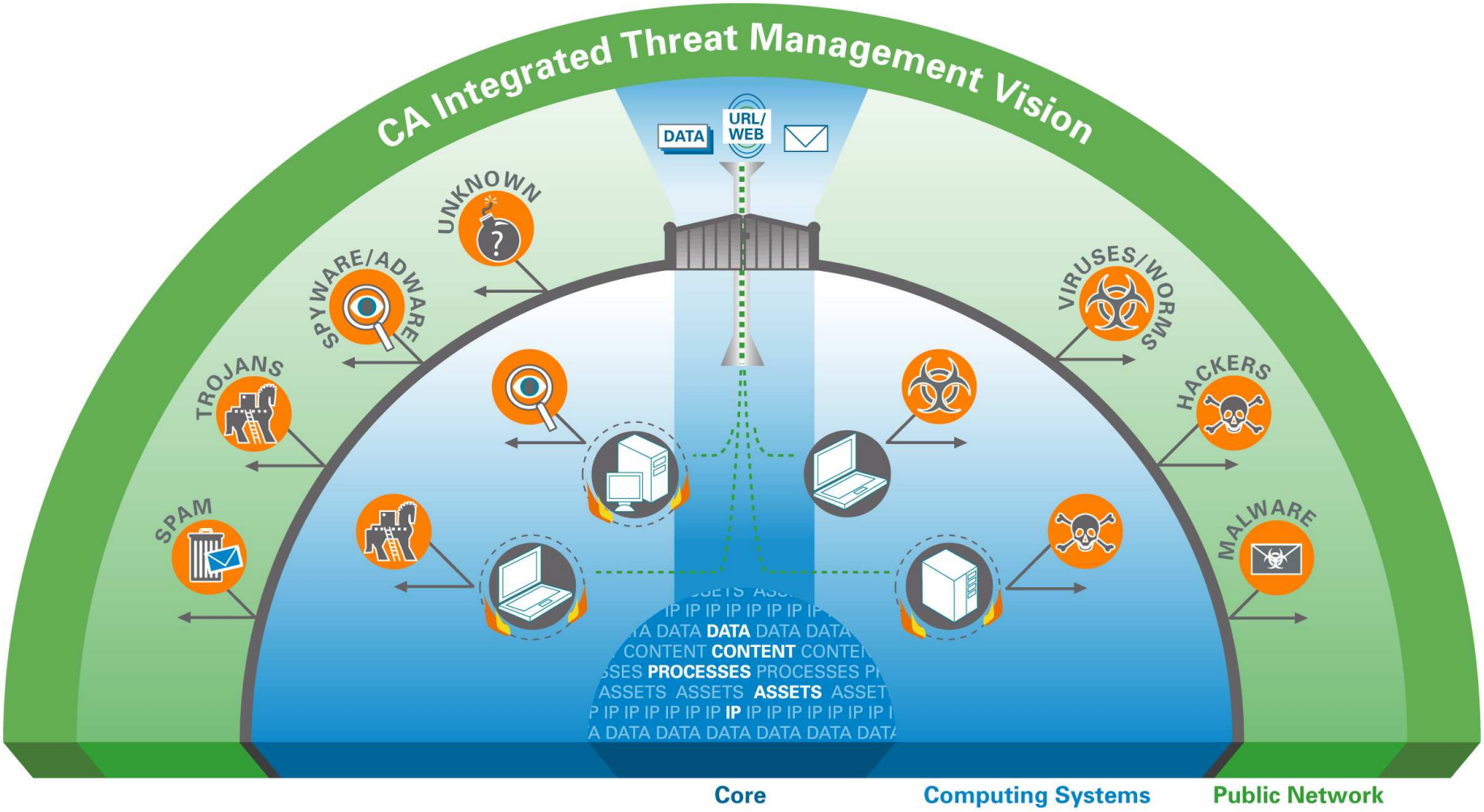
**Zdroj útoků**

- Díry v operačním systému a aplikacích
- Stahování dat z webu
- ActiveX, Java, skripty
- Přílohy emailů
- Přibalený software k freewaru a sharewaru
- Nezabezpečené Wireless Access Points
- Nezabezpečená sdílení (shares)

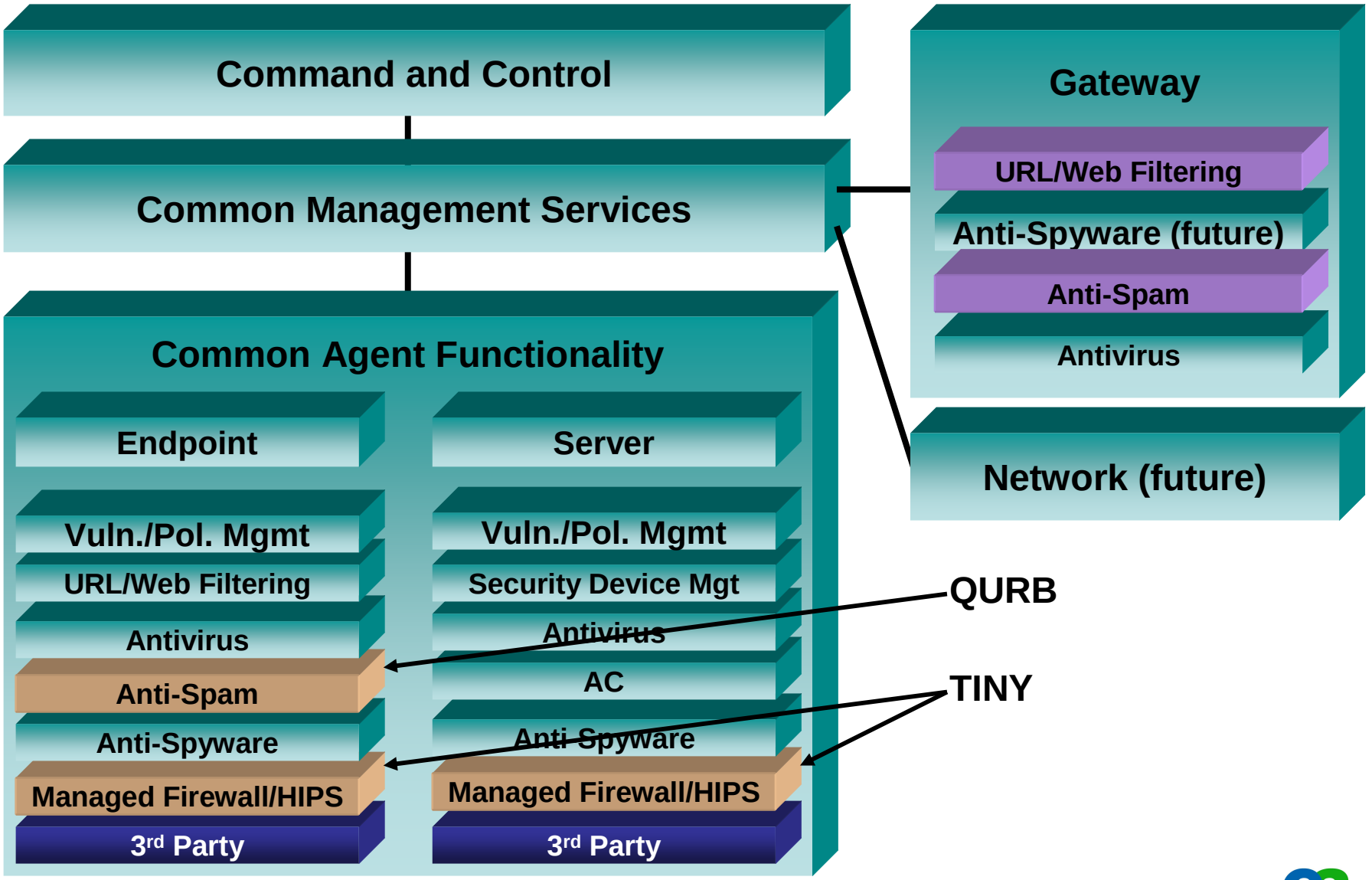
# Nechtěný software

- Adware
- Backdoor
- Browser Helper Objects
- Browser Hijackers
- Downloaders
- Droppers
- Keyloggers
- Password Crackers
- Remote Access Trojans
- Rootkits
- Spyware
- Trojans
- Viruses
- Worms

# CA ITM Vision

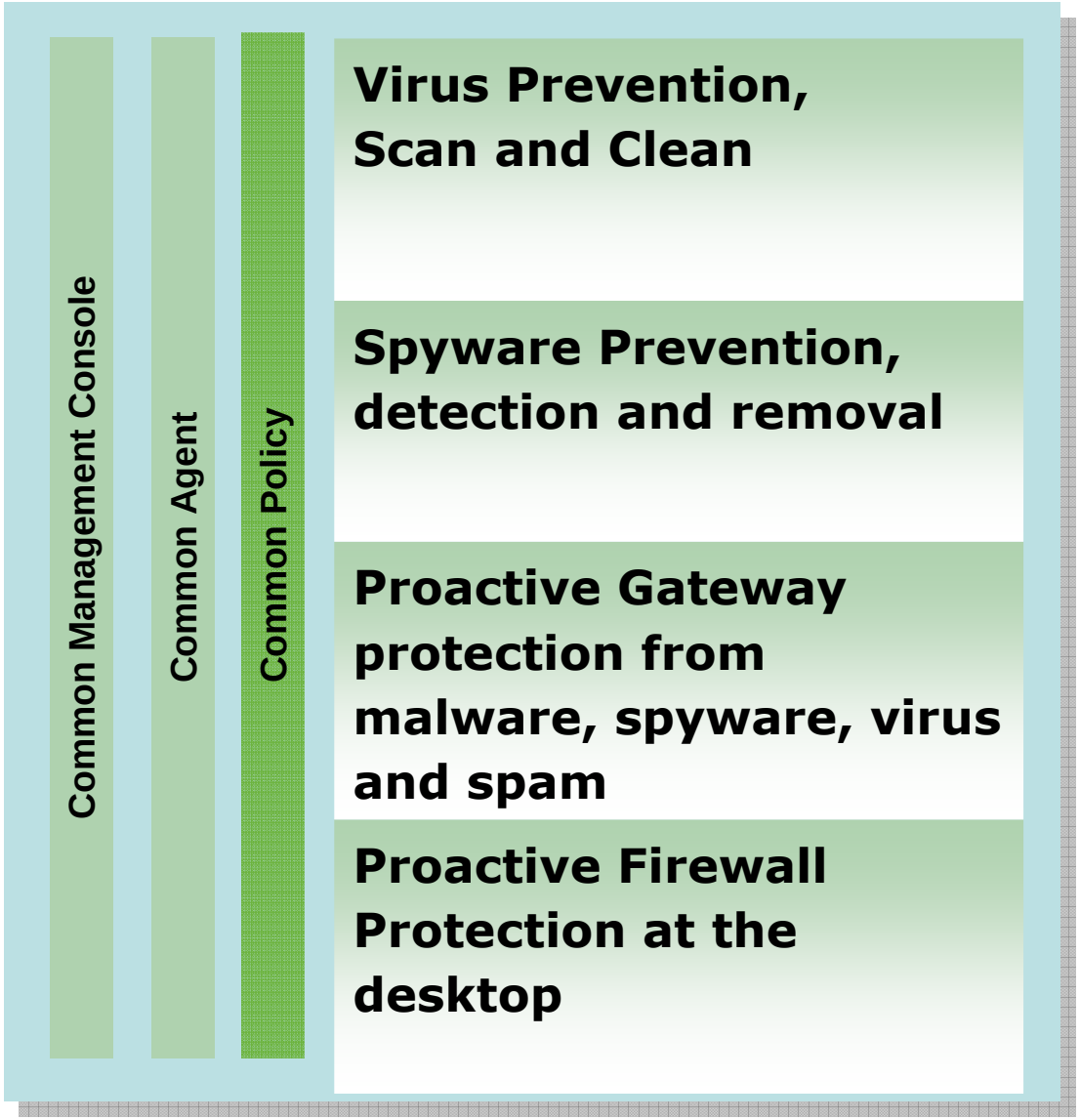


# CA ITM Vision



# CA ITM Vision

**CA Integrated Threat Manager Suite**



# Co přináší CA ITM

- **Standardní management**
  - Jedna infrastruktura managementu pro všechny ITM řešení
  - Standardní webové management prostředí
  - Standardní nasazení, politiky a reporting
- **Komplexní před bezpečnostními hrozbami**
  - Viry, červy, trójské koně
  - Spyware
  - Spam
  - Filtrování webu
  - Phishing
- **Modulární komponenty**
  - Samostatné moduly
  - Integrovaná řešení
  - Komplexní řešení

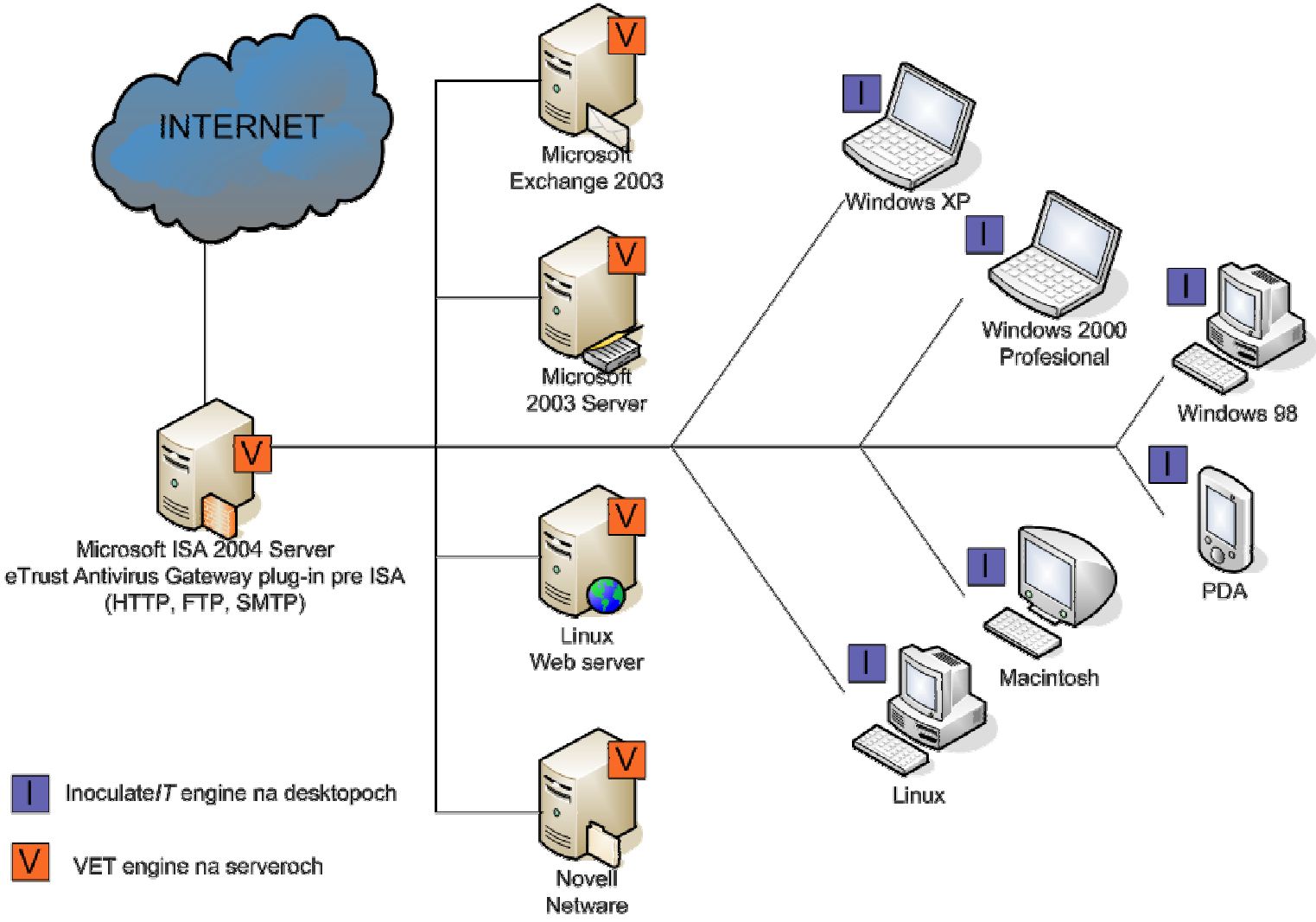
# Co přináší CA ITM

- **Zajištění Business Continuity**
  - Zvýšený důraz na management a řízení
  - Minimální implementační a adaptační issues
  - Snížení doby downtime
- **Snížení rizik**
  - Poskytnutí proaktivního managementu bezpečnostních rizik
- **Kontrola nákladů & ROI**
  - Poskytnutí standardní infrastruktury
  - Zefektivnění managementu
  - Redukování dopadu na implementace a adaptace

# Klíčové vlastnosti CA ITM

- Antivirová ochrana PC, serverů, sítí
- Dva nezávislé antiviry (Inoculan, Vet)
- Ochrana jednorázovou kontrolou i real-time
- Ochrana komunikačních bran (SMTP, POP3)
- Podpora MS Exchange a Lotus Domino
- Podpora řady operačních systémů
  - Windows, Linux, NetWare,  Pocket PC

# Koncept dvou antivirů

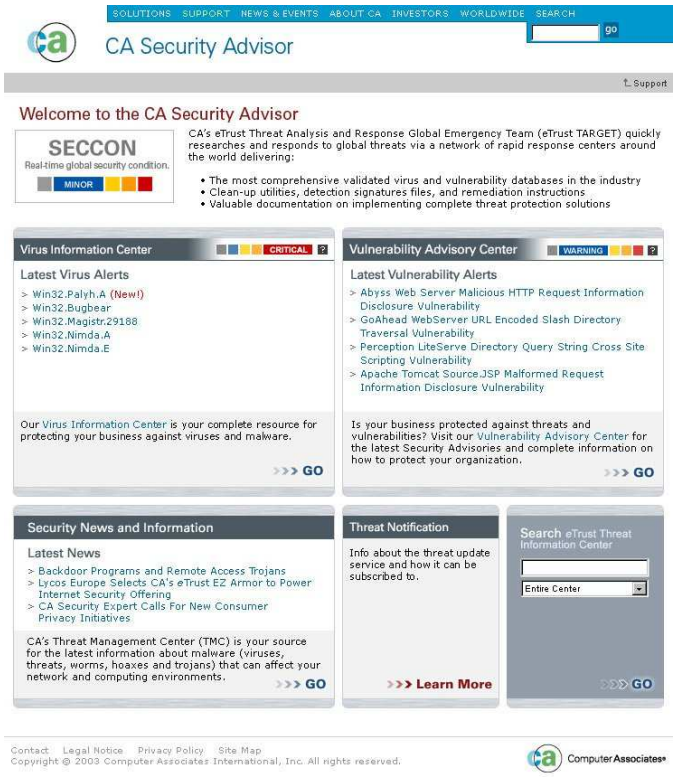


# Klíčové vlastnosti CA ITM

- Centrální instalace a update
- Centrální správa
- Centrální řízení politik práv
- Efektivní distribuce aktualizací
  - podpora interních distribučních serverů
- Centrální reporty a alerty

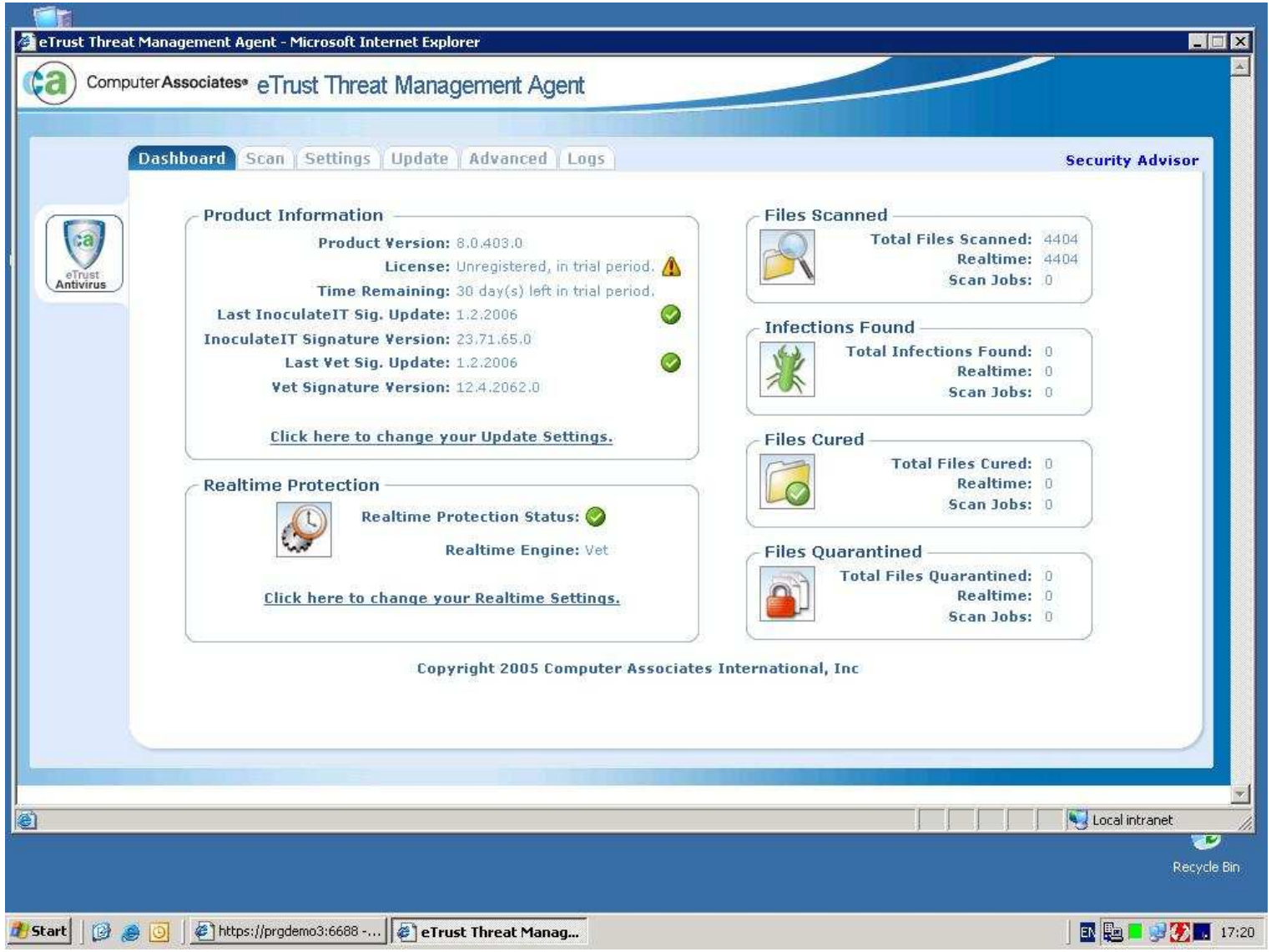
# CA Security Advisory Team

- 24x7 dohled nad bezpečnostními hrozbami
- Zdroj bezpečnostních informací od roku 1987
- Petentovaný proces pro výzkum, testování a kontrolu bezpečnostních rizik
- Výzkem z více jak 400 různých zdrojů
- Bezpečnostní support pro bezepčnostní rizika, viry, vniknutí a prevenci vzniku rizik
- Poradní tým pro Common Vulnerability Exposure Organization (CVE),  Infragard, Virus Bulletin

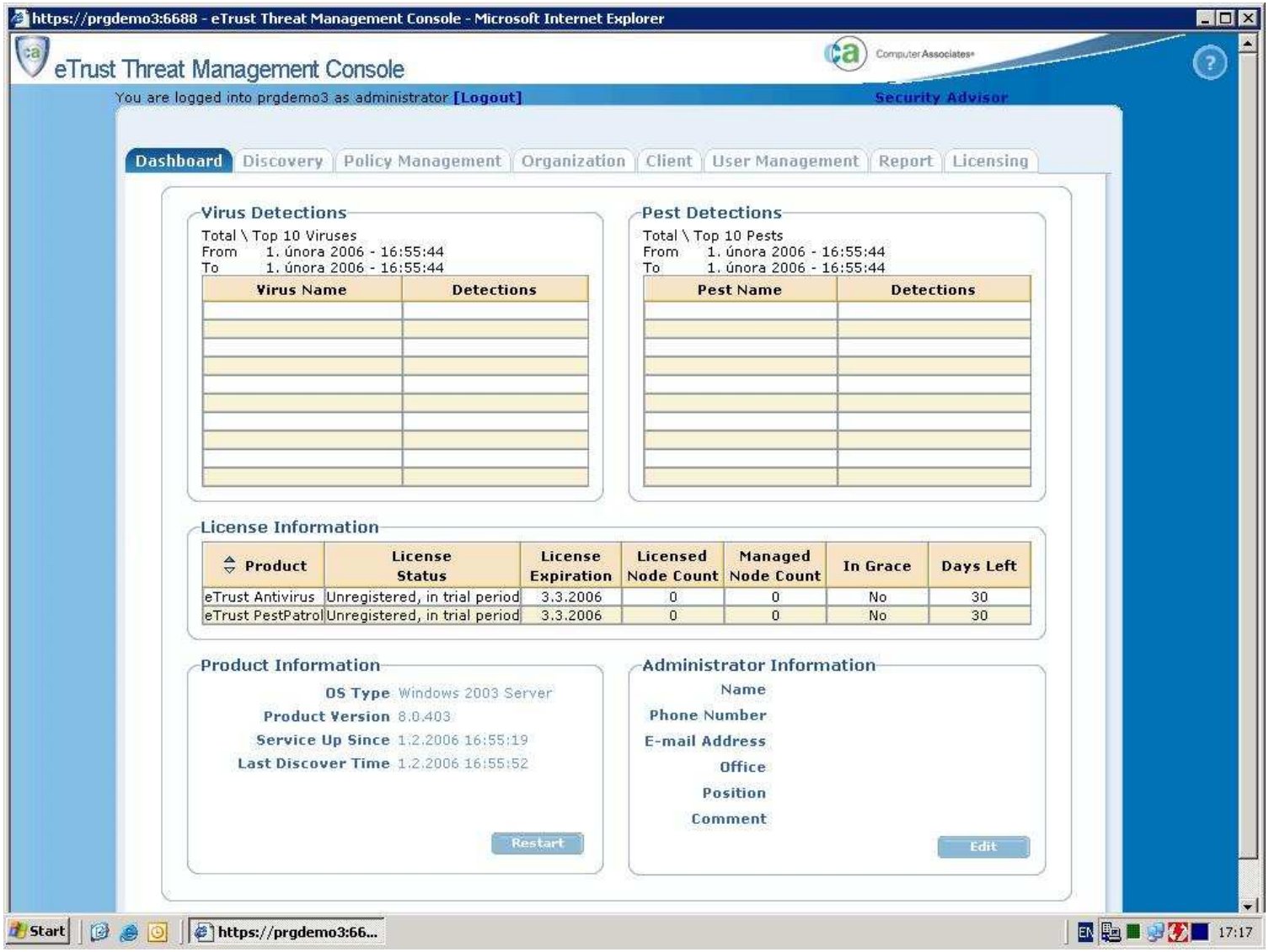



***virus@ca.com***

# CA ITM Agent



# CA ITM Server Console



# Kompatibilita

- Windows 95/98/Me
- Windows XP/NT/2000/2003
- Windows 2003 64 bit
- UNIX (Solaris,HP-UX)
- Linux (RedHat, SUSE)
- Linux for OS390, zSeries
- PalmOS
- Microsoft Pocket PC 2002/2003/Smartphone
- Macintosh OS X
- Novell NetWare 4.2, 5.x, 6.x
- Microsoft Exchnage 5.5, 2000, 2003
- Lotus Notes/Domino
- Plug-in CVP firewall
- Plug-in ISA server

# Licence

**Jedna licence obsahuje**

- CA ITM for Desktops, Servers
- CA Antivirus for PDA
- CA Antivirus for Groupware
  - Microsoft Exchange
  - Lotus Notes/Domino
- CA Antivirus Gateway edition

# Shrnutí

- Komplexní bezpečnostní řešení s jednoduchým licencováním
- Řešení pro stanice, servery, PDA, appliance
- Dva antiviry, anti-spyware/adware
- Pravidelné denní aktualizace
- Podpora široké škály operačních systémů
- Centrální řízení a správa
- Centrální reporty