



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, keyloggers, 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

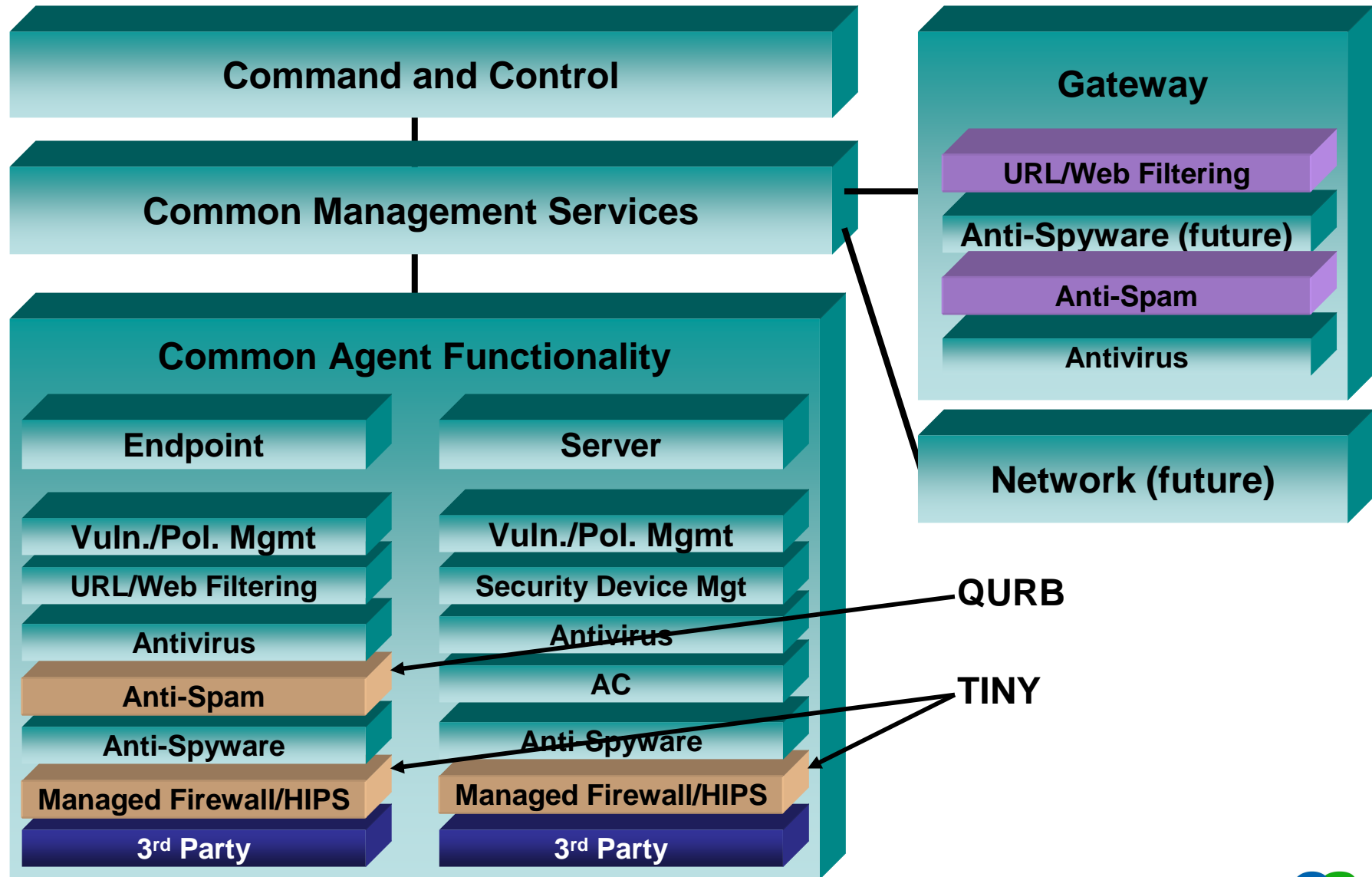
Zdroj útoků

- 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

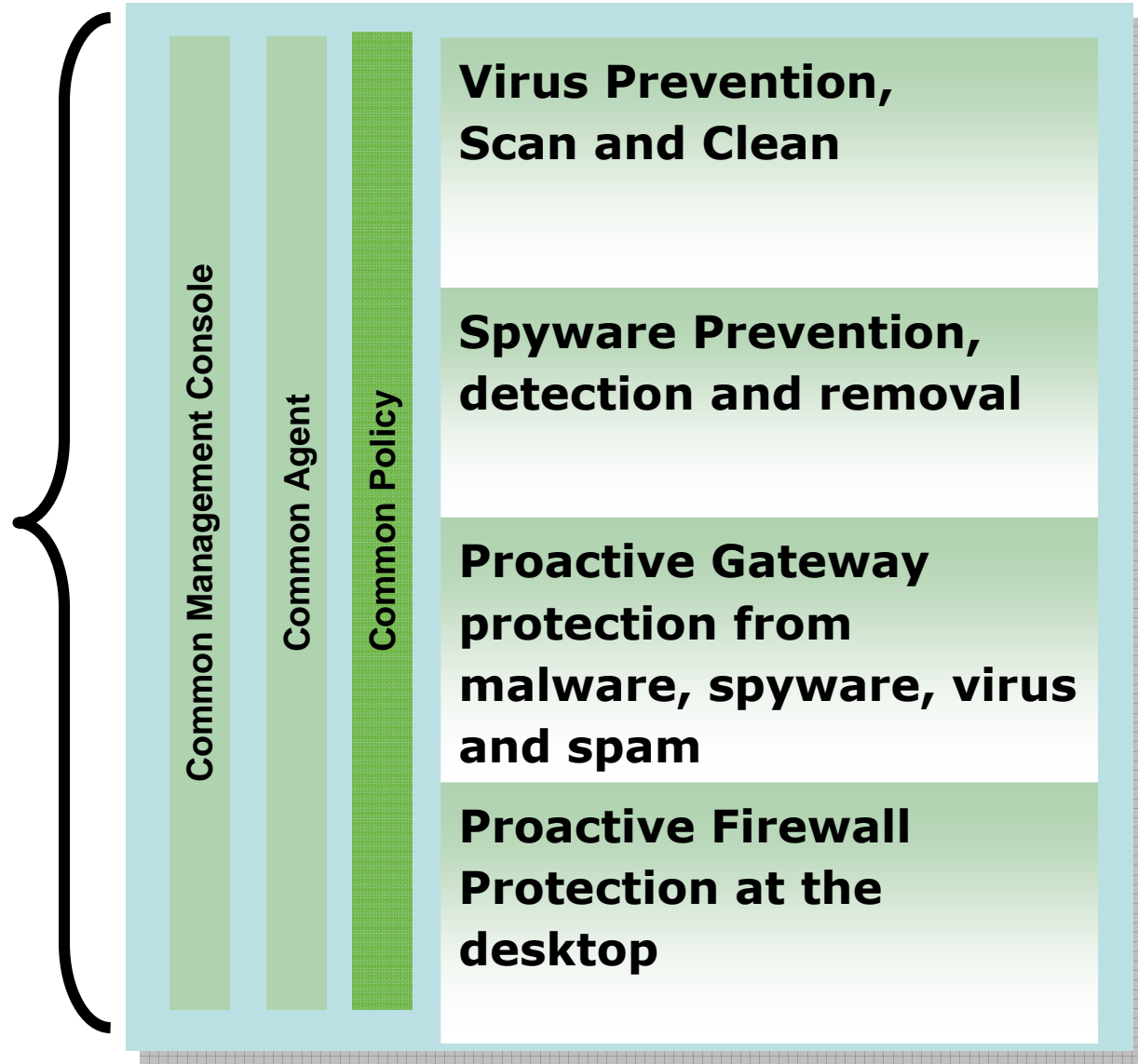
- Adware
- Backdoor
- Browser Helper Objects
- Browser Hijackers
- Downloaders
- Droppers
- Keyloggers
- Password Crackers
- Remote Access Trojans
- Rootkits
- Spyware
- Trojans
- Viruses
- Worms

CA ITM Vision



CA ITM Vision

**CA 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

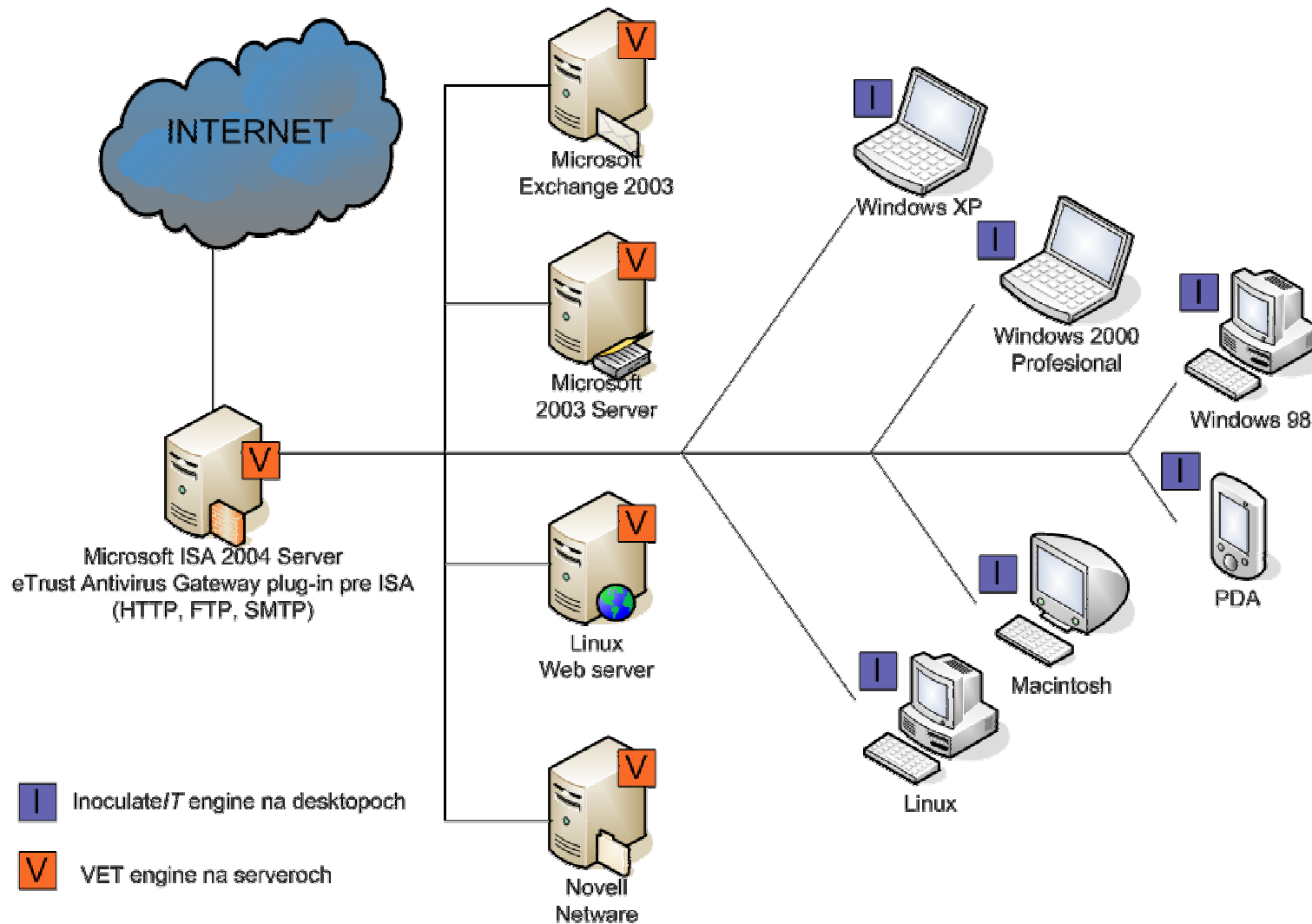
Co přináší CA ITM

- **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
- Patentovaný proces pro výzkum, testování a kontrolu bezpečnostních rizik
- Výzkem z více jak 400 různých zdrojů
- Bezpečnostní support pro bezpečnostní rizika, viry, vniknutí a prevenci vzniku rizik
- Poradní tým pro Common Vulnerability Exposure Organization (CVE), Infragard, Virus Bulletin

The screenshot shows the CA Security Advisor website. At the top, there is a navigation bar with links for SOLUTIONS, SUPPORT, NEWS & EVENTS, ABOUT CA, INVESTORS, and WORLDWIDE, along with a search bar. The main content area is titled "Welcome to the CA Security Advisor" and features a "SECCON" section with a "Real-time global security condition" indicator showing "MINOR" severity. Below this, there are two main columns: "Virus Information Center" and "Vulnerability Advisory Center". The Virus Information Center lists "Latest Virus Alerts" such as Win32.Polyh.A (New!), Win32.Bugbear, Win32.Magistr.29188, Win32.Nimda.A, and Win32.Nimda.E. The Vulnerability Advisory Center lists "Latest Vulnerability Alerts" such as Abyss Web Server Malicious HTTP Request Information Disclosure Vulnerability, GoAhead WebServer URL Encoded Slash Directory Traversal Vulnerability, Perception LiteServe Directory Query String Cross Site Scripting Vulnerability, and Apache Tomcat Source.JSP Malformed Request Information Disclosure Vulnerability. There are also sections for "Security News and Information" and "Threat Notification". At the bottom, there is a footer with contact information and the CA logo.

virus@ca.com



CA ITM Agent

The screenshot displays the CA ITM Agent web interface within a Microsoft Internet Explorer browser window. The browser title is "eTrust Threat Management Agent - Microsoft Internet Explorer". The page header includes the CA logo and "Computer Associates® eTrust Threat Management Agent".

The main content area is divided into several sections:

- Dashboard** (selected), Scan, Settings, Update, Advanced, Logs
- Security Advisor** (top right)
- Product Information**:
 - Product Version: 8.0.403.0
 - License: Unregistered, in trial period. ⚠️
 - Time Remaining: 30 day(s) left in trial period.
 - Last InoculateIT Sig. Update: 1.2.2006 ✓
 - InoculateIT Signature Version: 23.71.65.0
 - Last Vet Sig. Update: 1.2.2006 ✓
 - Vet Signature Version: 12.4.2062.0
 - [Click here to change your Update Settings.](#)
- Realtime Protection**:
 - Realtime Protection Status: ✓
 - Realtime Engine: Vet
 - [Click here to change your Realtime Settings.](#)
- Files Scanned**:
 - Total Files Scanned: 4404
 - Realtime: 4404
 - Scan Jobs: 0
- Infections Found**:
 - Total Infections Found: 0
 - Realtime: 0
 - Scan Jobs: 0
- Files Cured**:
 - Total Files Cured: 0
 - Realtime: 0
 - Scan Jobs: 0
- Files Quarantined**:
 - Total Files Quarantined: 0
 - Realtime: 0
 - Scan Jobs: 0

Copyright 2005 Computer Associates International, Inc

The taskbar at the bottom shows the Start button, several application icons, and the active window "eTrust Threat Manag...". The system tray on the right shows "Local intranet" and "Recycle Bin". The system clock shows "17:20".

CA ITM Server Console

The screenshot displays the CA ITM Server Console interface. At the top, the browser address bar shows 'https://prgdemo3:6688 - eTrust Threat Management Console - Microsoft Internet Explorer'. The page header includes the CA logo and 'Computer Associates'. A status bar indicates 'You are logged into prgdemo3 as administrator [Logout]' and 'Security Advisor'. Navigation tabs include Dashboard, Discovery, Policy Management, Organization, Client, User Management, Report, and Licensing. The main content area is divided into several sections:

- Virus Detections:** A table showing 'Total \ Top 10 Viruses' with columns for Virus Name and Detections. The table is currently empty.
- Pest Detections:** A table showing 'Total \ Top 10 Pests' with columns for Pest Name and Detections. The table is currently empty.
- License Information:** A table with columns: Product, License Status, License Expiration, Licensed Node Count, Managed Node Count, In Grace, and Days Left.
- Product Information:** A section showing OS Type (Windows 2003 Server), Product Version (8.0.403), Service Up Since (1.2.2006 16:55:19), and Last Discover Time (1.2.2006 16:55:52). A 'Restart' button is present.
- Administrator Information:** A section with fields for Name, Phone Number, E-mail Address, Office, Position, and Comment. An 'Edit' button is present.

The Windows taskbar at the bottom shows the Start button, several icons, and the address bar with 'https://prgdemo3:66...'. The system tray on the right shows the date and time as 17:17.

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

