

© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com



"The staff are healthy enough,
it's the computers that keep
getting a virus!"

Anti Virus is a Commodity
Stephen Osler
Nclose



nclose
- security within -

Who Nclose is?

- Security Specific Service Provider
- Vendor Agnostic
- Specialist Products (Kaspersky, Websense, Juniper, eEye Digital Security, Utimaco)



Agenda

- Traditional vs Technological Commodity
- AntiVirus how things have changed since 2002
- Factors that assisted in the commoditization of Anti Virus
- Factors to considered when looking at an alternative AntiVirus



Traditional vs Technological Commodity

Traditional

- A commodity is anything for which there is demand, but which is supplied without qualitative differentiation across a market. In other words, copper is copper. Rice is rice. (Wikipedia)
- Commoditization occurs as a goods or services market loses differentiation across its supply base.(Wikipedia)

Technological

- Solutions where the leading products are interchangeable.
- Vendors compete on extended or niche capabilities.
- Vendors compete on solution price.
- There is no barrier to user entry-level adoption





AntiVirus for XP in 2002



www.virusbtn.com

- 1) Alwil (Avast!)
- 2) Authentium (formerly Command Software Systems)
- 3) CAT QuickHeal
- 4) **CA eTrust**
- 5) Doctor Web (formerly DialogueScience)
- 6) **Eset (NOD32)**
- 7) **F-Secure**
- 8) **Frisk (F-Prot)**
- 9) GDATA
- 10) GeCAD (RAV)
- 11) **Grisoft (AVG)**
- 1) Hauri (ViRobot)
- 2) **Kaspersky**
- 3) Leprechaun VirusBuster II.
- 4) **McAfee Inc. (formerly Network Associates)**
- 5) **Norman**
- 6) **Panda Software**
- 7) **Softwin (BitDefender)**
- 8) **Sophos**
- 9) **Trend Micro (PC-cillin)**
- 10) VirusBuster



nclose
- security within -



AntiVirus for XP in 2008



www.virusbtn.com

- | | | |
|------------------------------------|--|---|
| 1) Agnitum | 1) Webroot AntiVirus | 1) PC Tools AntiVirus |
| 2) AhnLab | 2) Frisk F-PROT Antivirus | 2) Fortinet FortiClient |
| 3) Alwil | 3) F-Secure Internet Security | 3) Proland Software |
| 4) ArcaBit | 4) F-Secure Protection Services | 4) PC Tools Spyware Doctor |
| 5) AVG (Grisoft) | 5) GDATA AntiVirus | 5) Quick Heal AntiVirus |
| 6) Avira | 6) K7 Total Security | 6) Redstone Redprotect |
| 7) BitDefender (SOFTWIN) | 7) Kaspersky Anti-Virus | 7) Rising Antivirus |
| 8) Bullguard | 8) Kingsoft | 8) Sophos Endpoint Security & Control. |
| 9) CA AntiVirus | 9) McAfee | 9) Symantec Endpoint Protection |
| 10) CA eTrust | 10) MWTI eScan Internet | 10) Trustport Antivirus |
| 11) eEye Blink Professional | 11) Norman Security Suite | 11) VirusBuster Professional |
| 12) ESET NOD32 | 12) NWI | 12) Webroot AntiVirus with AntiSpyware |



nclose
- security within -

Gartner Reports 2006 - 2007

- Gartner Magic Quadrant for AntiVirus August 2006

- CA
- F-Secure
- McAfee
- Sophos
- Symantec
- Trend Micro

- Gartner Magic Quadrant for End Point Protection December 2007

- Big Fix
- Bit 9
- CA
- Check Point
- eEye
- F-Secure
- IBM (ISS)
- Kaspersky
- LAN Desk
- McAfee
- Microsoft
- Panda
- Sophos
- Symantec
- Trend Micro
- Webroot



Factors that assist in the Commoditisation of AntiVirus

- **Factor 1: Continuing criminalization of the Internet**
- Factor 2: Increased variety of malware and attack methods
- Factor 3: Software Consolidation (Design problems)
- Factor 4: Competition

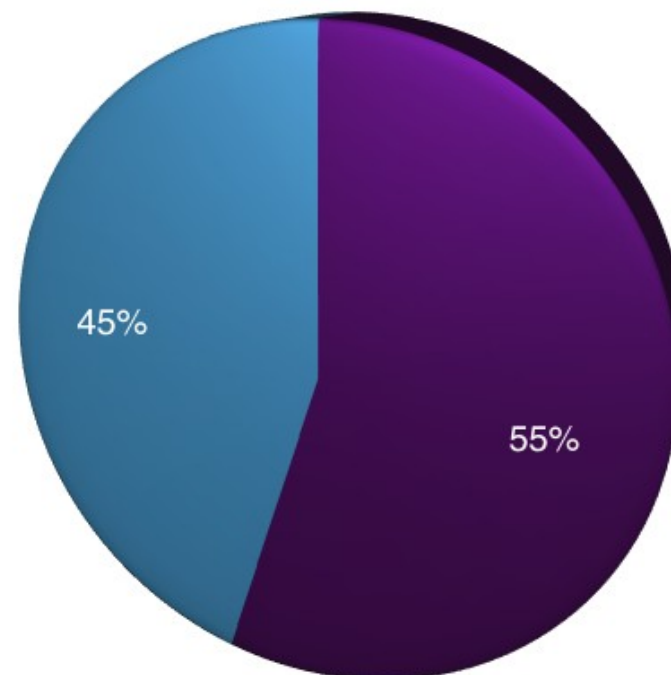


Factor 1: Continuing criminalization of the Internet

- The size of the community (the bigger it is, the higher the number of potential and actual threats)
- The ability of law enforcement bodies (e.g. the police) to investigate crimes and imprison the perpetrators
- £200Bill per annum
- Web 2.0

Total Vulnerabilities reported in SANS @RISK Data From Nov 2006 - Oct 2007

● Web Application Vulnerabilities ● Other Vulnerabilities



Factors that assist in the Commoditisation of AntiVirus

- Factor 1: Continuing criminalization of the Internet
- **Factor 2: Increased variety of malware and attack methods**
- Factor 3: Software Consolidation (Design problems)
- Factor 4: Competition



Factor 2: Increased variety of malware and attack methods

- Network worms
- A wide range of Trojan programs, including Spyware
- AdWare
- Network attacks
- Malicious application of legitimate programs (such as keyloggers and remote administration utilities)
- A wide range of spam, from begging emails to blackmail
- Phishing, Pharming or Spear Phishing a clearly differentiated type of financial scam
- Ransom-ware
- <http://isc.sans.org>



Factors that assist in the Commoditisation of AntiVirus

- Factor 1: Continuing criminalization of the Internet
- Factor 2: Increased variety of malware and attack methods
- **Factor 3: Software Consolidation (Design problems)**
- Factor 4: Competition



Factor 3: Product Consolidation

- Acquisition
 - Symantec
 - IMLogic - Instant Messaging Management.
 - Altiris - IT management software
 - Trend Micro
 - Provilla - Data Leakage Prevention
 - HijackThis - AntiSpyware
 - McAfee
 - Reconnex - Data Leakage Prevention
 - Safeboot - Encryption



Factors that assist in the Commoditisation of AntiVirus

- Factor 1: Continuing criminalization of the Internet
- Factor 2: Increased variety of malware and attack methods
- Factor 3: Software Consolidation (Design problems)
- **Factor 4: Competition**



Factor 4: Competition

- In Excess of 35 Commercial AV Vendors
- Software as a Service
- Software Authentication Services
- Software Whitelisting



Factors to considered when looking at an alternative AntiVirus

- Product Delivery
 - Managability
 - Proactiveness (Pattern File Updates)
 - Infrustrature
 - Road map (Past and Present)
- Partners Ability
 - Product Knowledge (Technical and Pre-sales)
 - Vendor relationships



Questions and Answers

- Thank you

