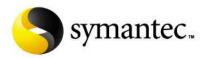


# **Antivirus Software Tests: What You Need to Know**

Sarah Gordon Senior Research Fellow Symantec Security Response







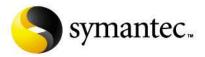
the fastest

best research

How do people evaluate antivirus software ????

best response

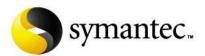
the best detection





#### Home users

- Recommendation
- Legacy software
- Price
- Box
  - Color
  - Certification Logos, Checkmarks, Awards on Box
- Test
  - Magazine & Commercial Testers>>logos, Academic tests>>results
    - ❖Some home users attempt to test
      - Bad idea

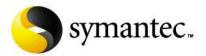




#### **Enterprise**

- Recommendation of friend
  - CTO talks to buddy at other company
  - Legacy software
- Price, TCO
- Box
  - Color of clothes on ad, trade show effective advertising
  - Certification logos, Checkmarks, Awards listed
- Test
  - Commercial, Private, Academic, Magazine, In-house

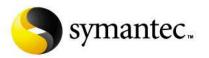






#### Why me?

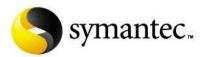
- Testing related experience
- Industry liaison
- Publications
- Academic





## Our mission: Put certification and testing of antivirus software into perspective

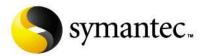
- Who is doing the testing
- What are they testing
  - What are they not testing?
- How are they testing
  - How are they not testing?
- What does this mean to you?
  - Some examples





#### **Tests are Important**

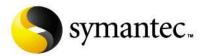
- What makes a Good Test?
  - Scientific
    - ❖ Valid, reliable reproducible
    - Documented, Peer-Reviewed
    - Sound Criteria and Methodology
  - Meaningful
    - The critical question: Does it measure something that is important to you
  - Doesn't matter how "in depth" it is if its not scientific and meaningful
  - Must have both to be of optimal value to the user.





#### The Teams – Big Pictures in Testing

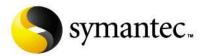
- University
- Commercial
- Independent
- Magazine Testers
- In-House





### The Players – Who is doing the Testing

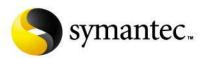
- Affiliations
- Qualifications & Experience





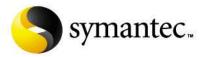
#### **The Game-Testing**

- The goal: Assessing performance
  - What is being tested
- The rules: Methods
  - How are they testing it
- The score: Interpretation
  - Pros and Cons
  - What does this mean to you?



#### Things to Consider

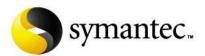
- Testing organization purpose
- Commercial/non-commercial aspects
  - Amount of Data to Process
    - Timing
    - In the Wild Tests
      - Zoo Tests
    - Detection, Disinfection
    - Malware, Trojan Horses
      - Polymorphics
      - Standard Test Sets
        - Common Infectors
      - False Positive Criteria
    - Weighting or lack thereof
      - Response Times
    - Synergistic holistic effect





#### Other Issues & Examples

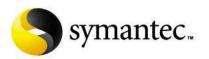
- Downstream usage of test results
- Typos, Real Discrepancies & Possible Explanations
- What is not being tested
- Comments from the field





#### **Closing thoughts**

- What is not tested is important
  - Response times are not so easy to test!
- What is tested is important (sometimes)
  - A products ability to detect all of the viruses in circulation is important.
  - A products ability to detect an obscure zoo virus sample is much less important.
  - What about the ability of a product to detect a virus that is within an archive?
  - The ability to detect a destructive worm coming into the network?
- System impact on detection and Synergistic/holistic effects can be very important.
  - Would non-AV specific solutions have stopped a particular threat?
  - Is the right response reconfiguration, firewall, or even user response?
- How is the information presented?





#### What does this mean to you?

- Tests are out there
- You are influenced by them
  - Directly
  - Indirectly
- They all have strengths, and weaknesses
- A good test is scientific and meaningful

Always keep that in mind