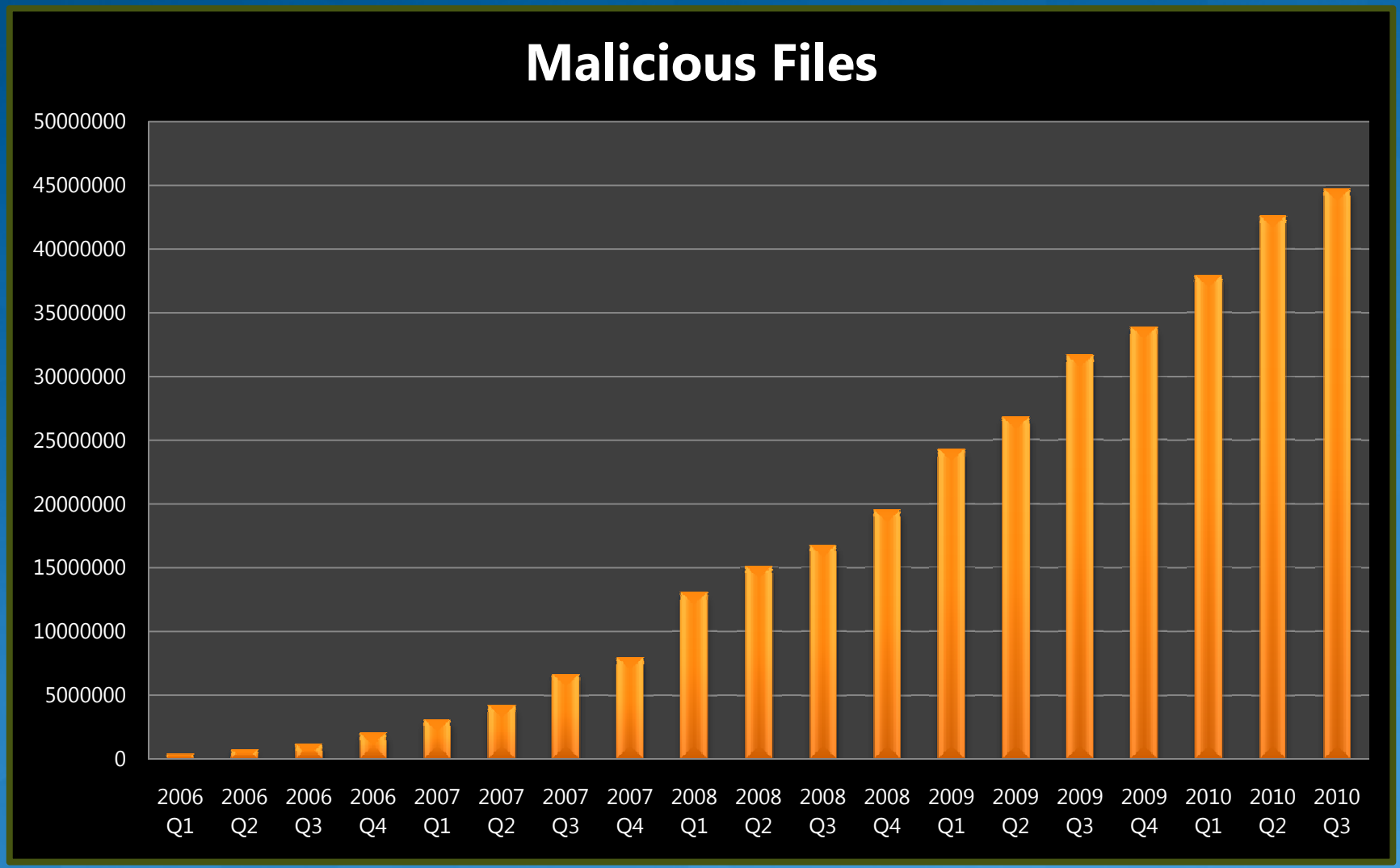
Telemetry Exchange and Industry Testing

Tony Lee
Jimmy Kuo

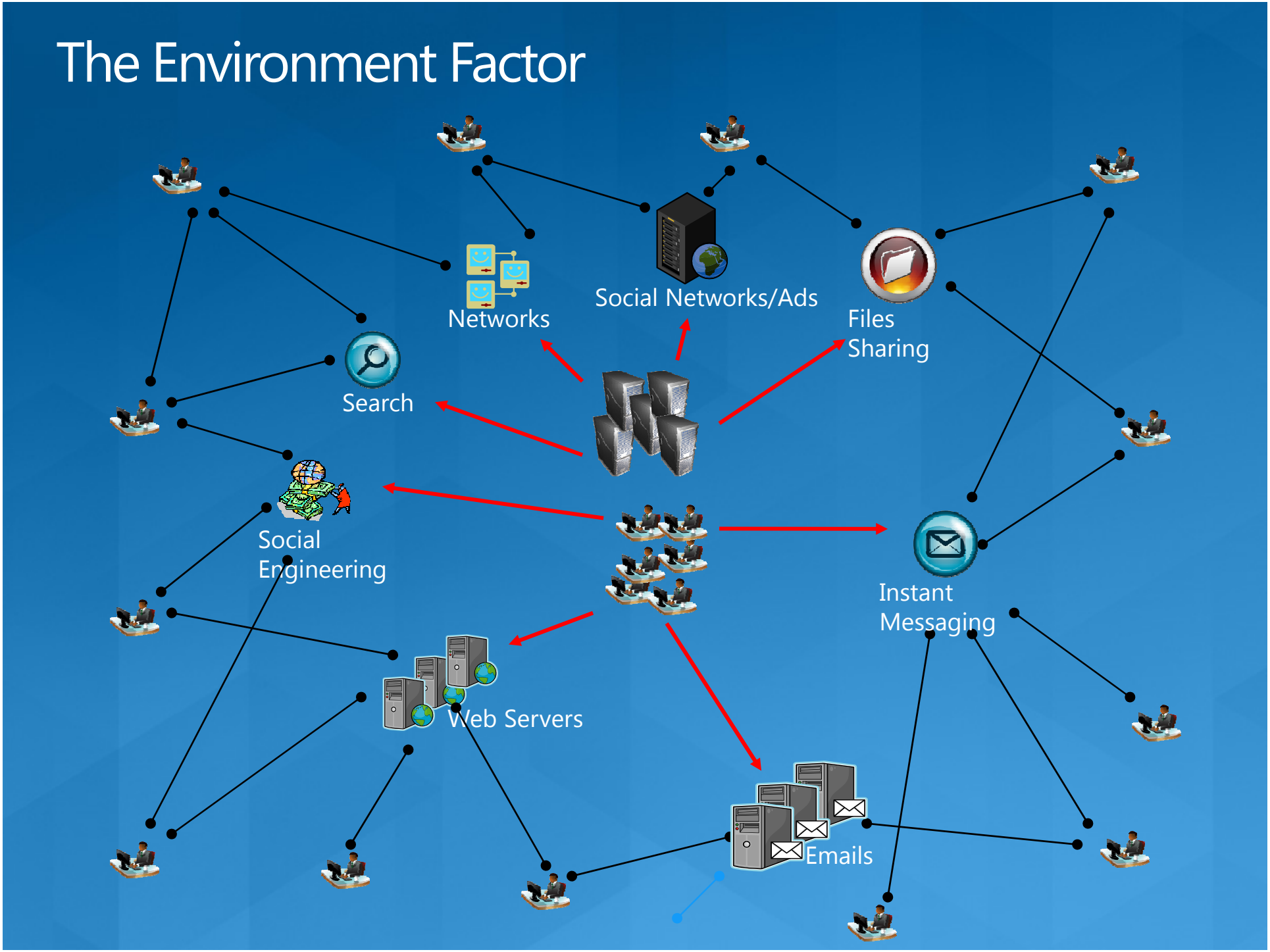
Malware Protection Center
Microsoft Corporation

The Number Factor



Source: Microsoft

The Environment Factor

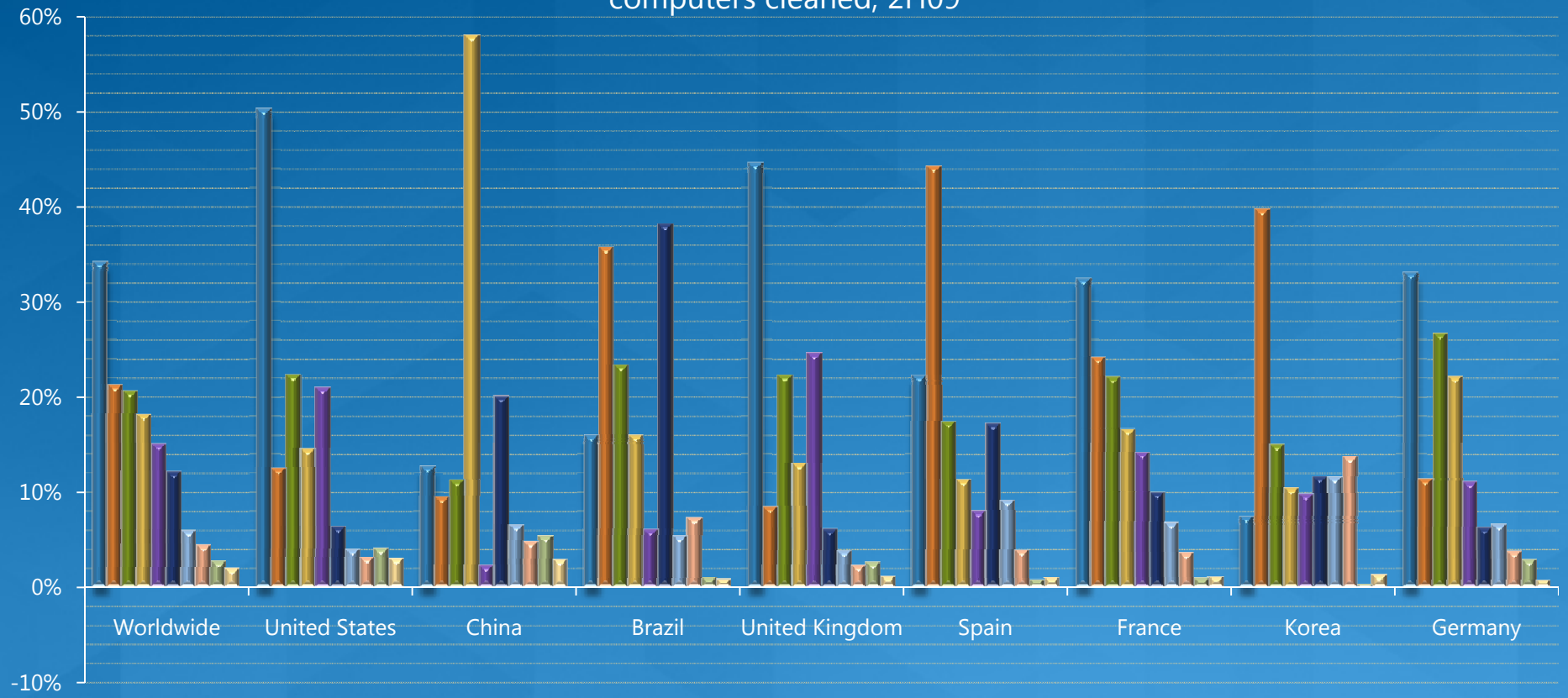


The Geographic Factor

Geographic trends

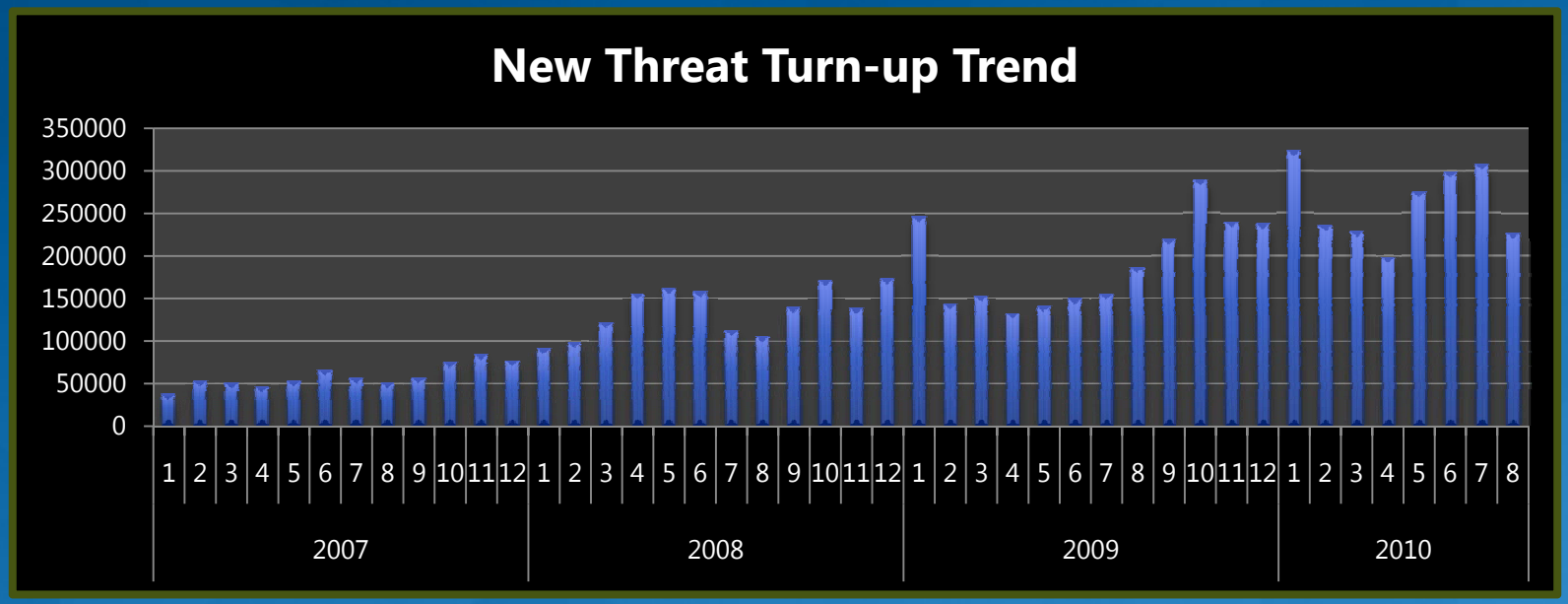
- Significant differences in threat patterns worldwide

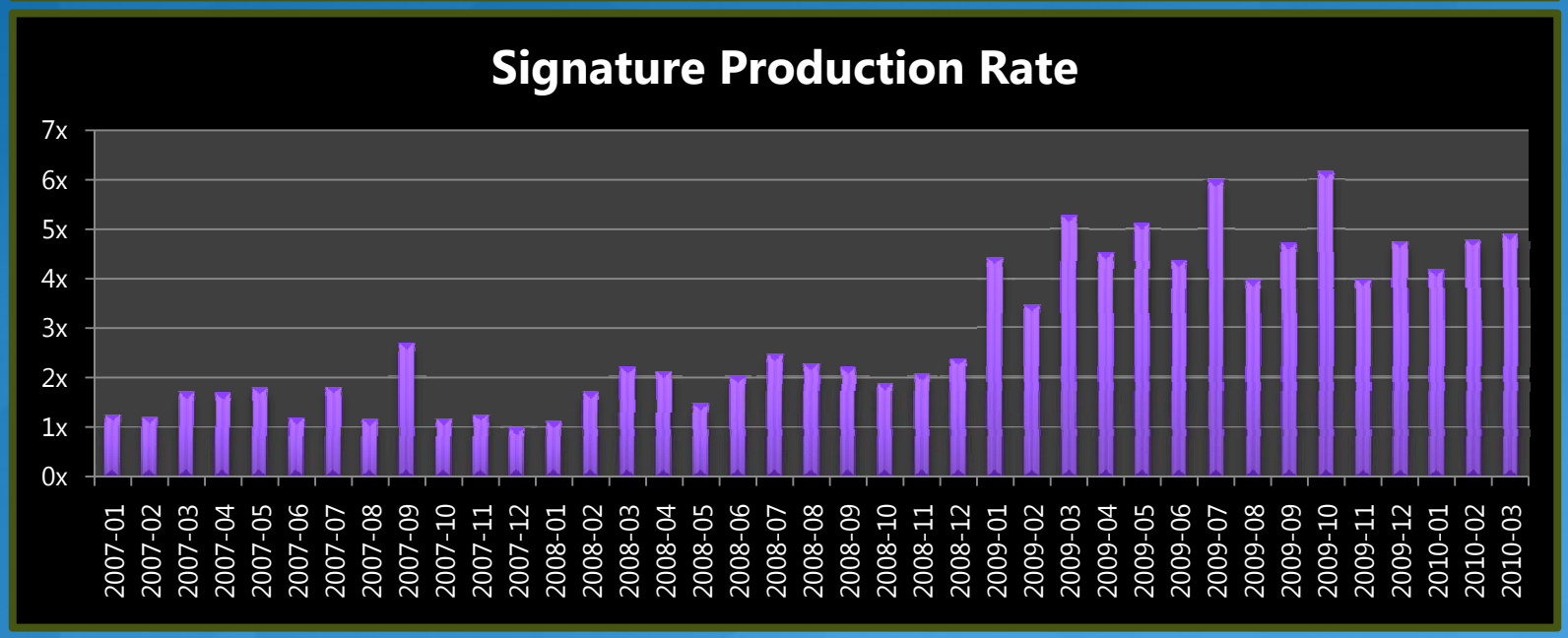
Threat categories worldwide and in eight locations around the world, by incidence among all computers cleaned, 2H09



Source: Microsoft SIR v8

Threat Cycle Factor





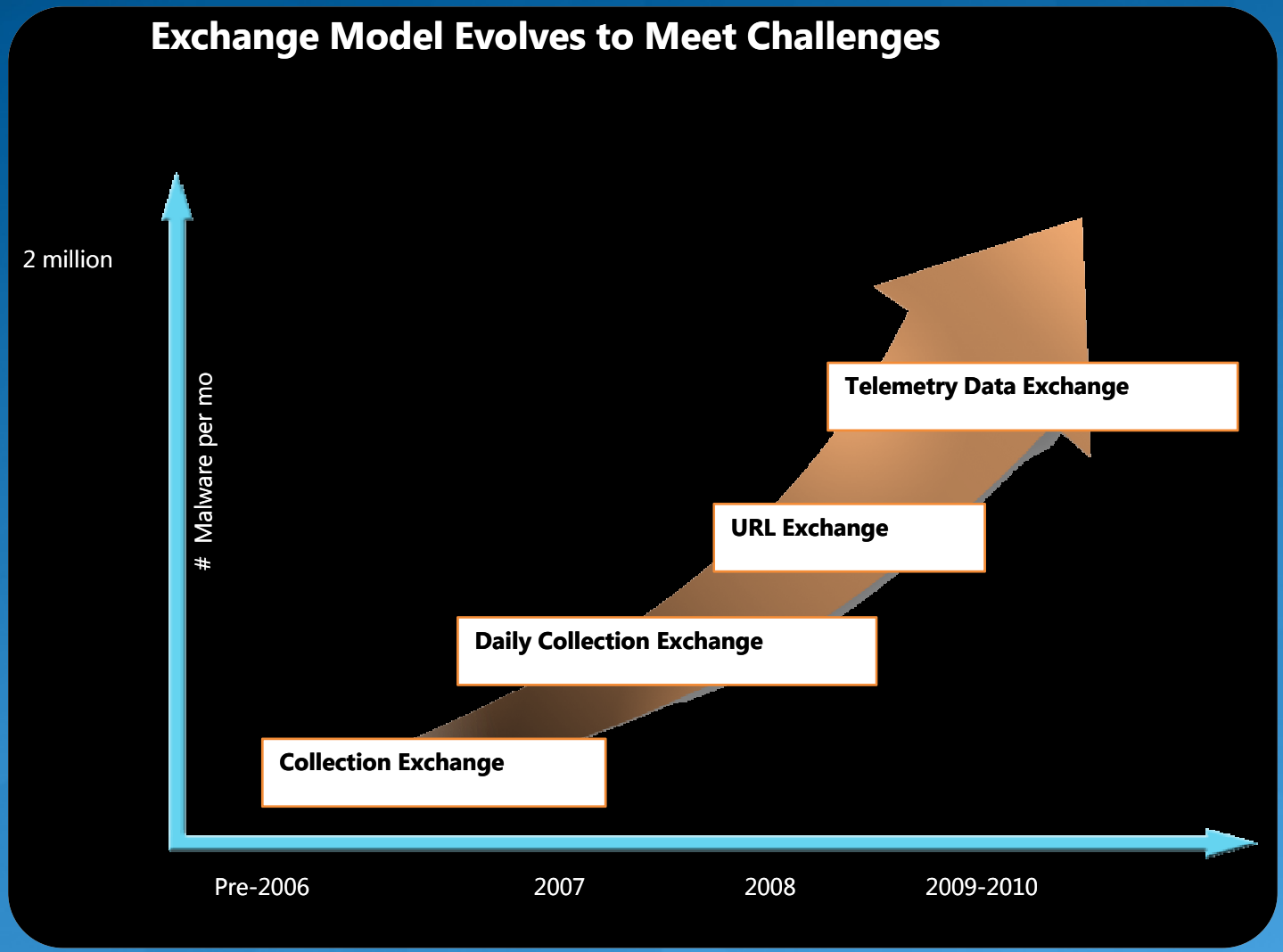
Complex Threat Landscape

- Large number of threats
- Diverse environment and attack vectors
- Geo-social and linguistic influences
- Shortening of Threat Cycle

Information Specialist

Effective Protection Across On-premise & Cloud

Evolution of Collaboration

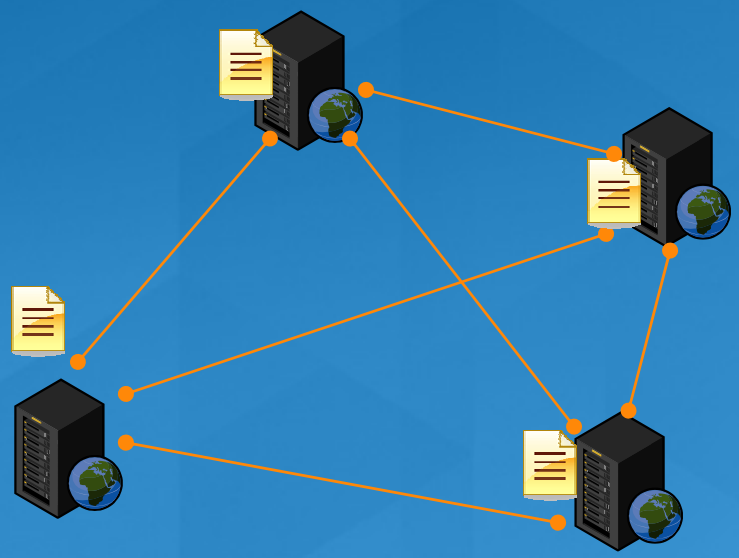


Challenges and Solutions

Challenges	Solutions
Lack of driving incentive and value	Promote adoption (up the stakes in the pot) Encourage shift in industry testing methodology toward incorporating telemetry data.
Technical Complexity	Educate, demonstrate Develop and share tools and proven methods

Data Exchanges in Action

- Industry forms working group – IEEE Industry Connection Security Group (ICSG)
- Focused on development of a XML based metadata sharing.
- Exchange are bi-lateral.



AVG
AV-Test
Cisco
McAfee
Microsoft
Panda
SonicWall
Symantec
Sophos
Trend
WebSense
and many others...

Data Exchanges in Action - Schema

http://grouper.ieee.org/groups/malware/malwg/Schema1.1/

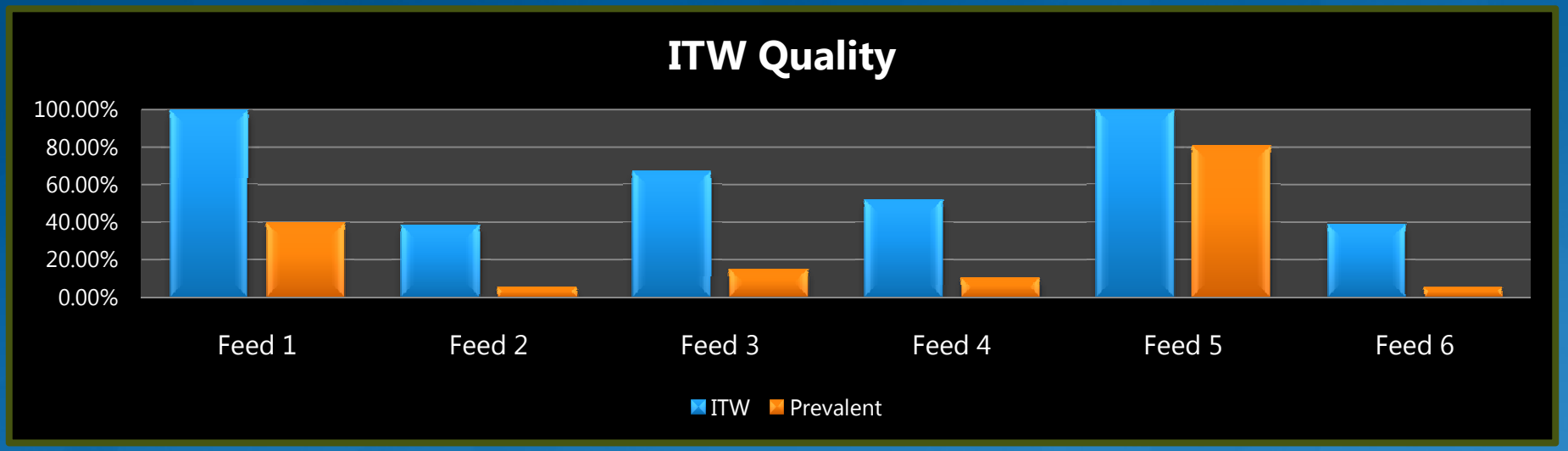
Detail schema documentation and help

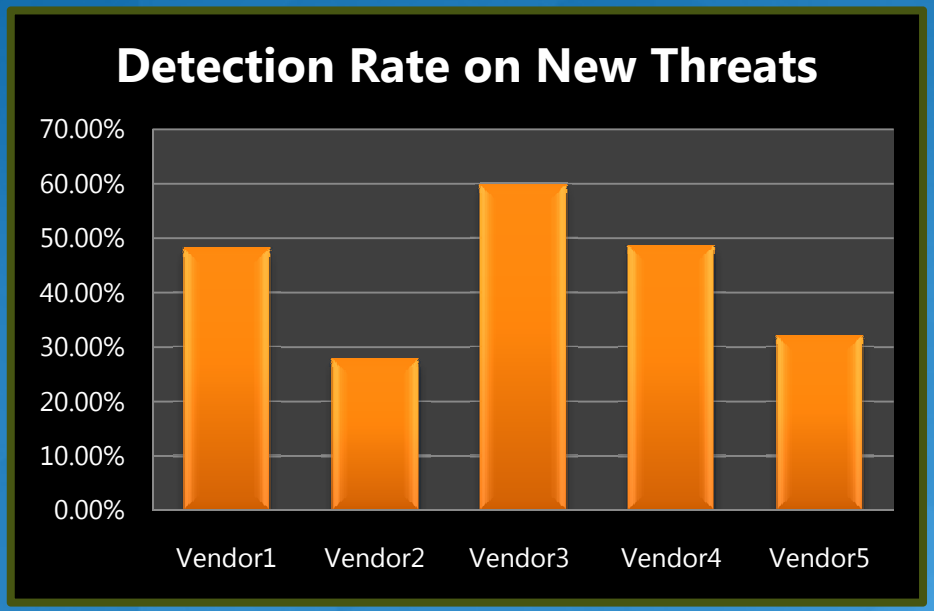
Data Exchanges in Action - Scenarios

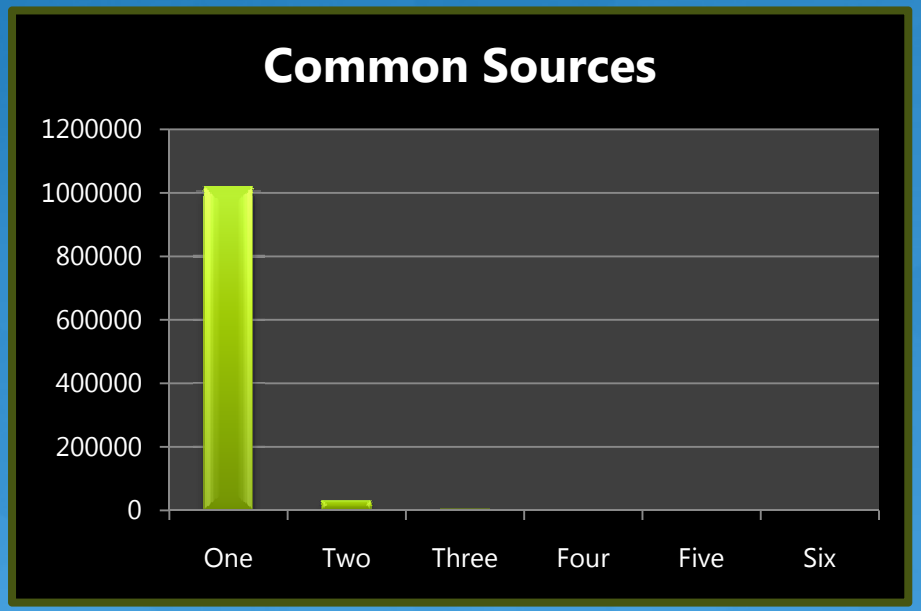
Scenarios

Dynamic Prevalence
Malware File Properties
Threat Classification
URL, IP, Domain
Region
And many others…

Data Exchange in Action – Case Study

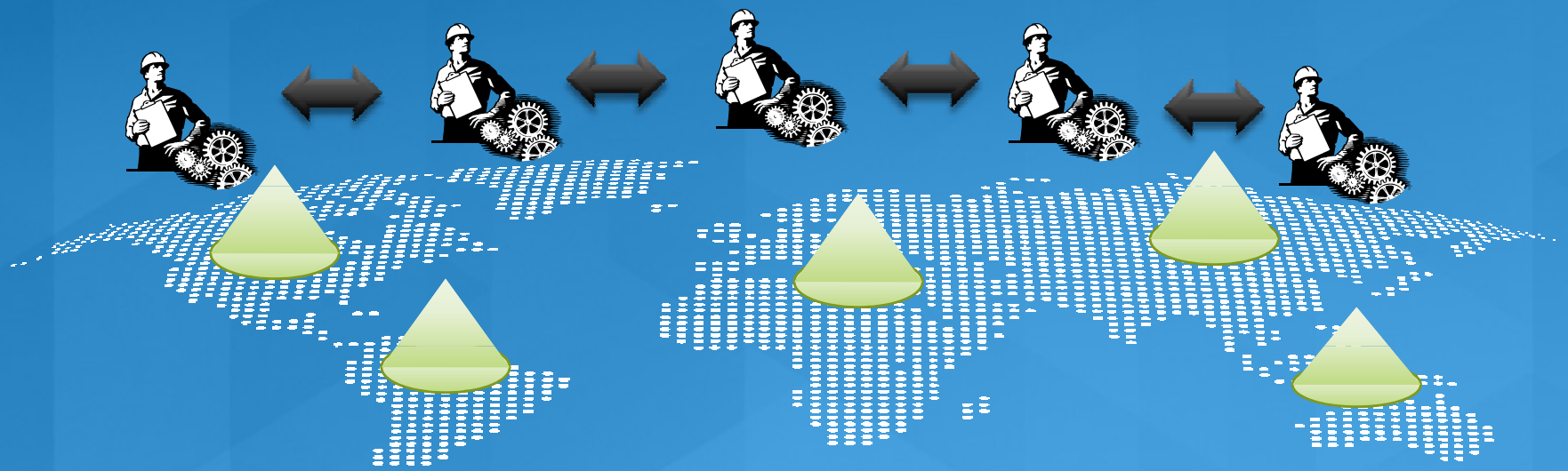






Data Exchange In Action

- Data feeds show promising value.
- Standard XML schema reduces cost/complexity, improve data representation.
- Share tools and experience

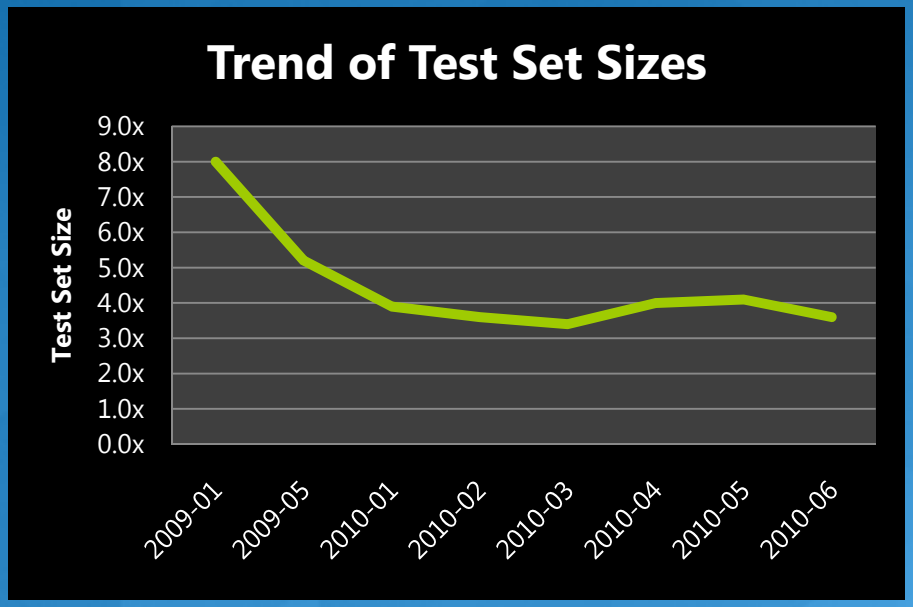


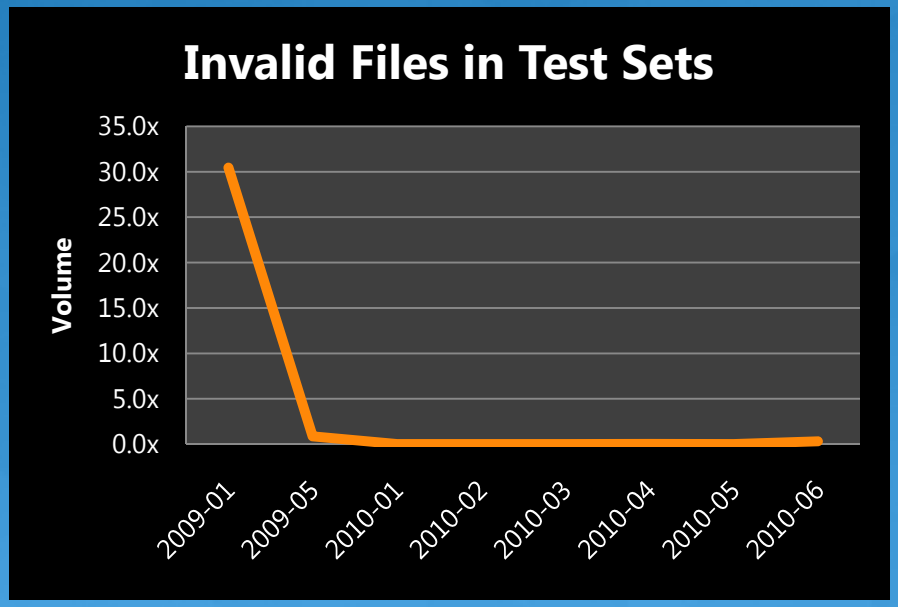
Industry Testing

Relevance Measure in Testing Methodology

- More samples ≠ Better test
- Be representative of what users really see
- Reflect product capability in user protection

Testers made substantial progress in refining test set quality, leveraging data feeds and tools from industry.





Industry Testing Cont.

Concerns	Solutions
Participants gaming test with faulty data	Collate data from different sources, prevent subset of feeds from dominating, not much different from samples.
Complexity in merging disparate data sources	IEEE ICSG Data Exchange Schema Source normalization
Lack of data sources Industry receptiveness to new tests	Need to take a step forward to set in positive feedback cycle. Add additional sub-test or create experimental test, for example, test with telemetry-base score. Work with IEEE ICSG, industry wants and welcomes changes.

What do these all mean to users

- AV products can better protect customers, benefited from threat intelligence sharing.
  - Signatures on “real” threats can go into the delivered sets. Less than real threats can have their signatures in the cloud.
- Product testing results are more indicative of protection performance in the field, i.e. what impacts the actual users.
- As test sets get smaller (full product tests), telemetry based sets become even more important.

The Importance of False Positives in Testing

How good is The Perfect AntiVirus?

- 100% detection!
- Never needs updating!
- VERY FAST!
- Low System Overhead!

Hypothetical Test Results

AV-Comparatives On-Demand Test Aug 2010: Tested

AV-Comparatives Proactive Test May: Advanced

AV-Comparatives Whole Product Test: Advanced+

AV-Test: 100% Protection and receive certification

PCSL Total Protection Test: 97% (if no files in clean set)

NSS: 100% detection of social engineering malware

Hypothetical Certification Results

ICSA: Fail!

West Coast Lab: Fail!

VB100: “20 years of trying, the VB100 continues to be out of its grasp. I don’t know why it continues to get satisfactory marks from testers, nor even why I continue to test it! I suppose it’s because it’s so easy to test. You can always stand by this product to say the same thing time after time.” -- John Hawes

The Perfect Antivirus

Kept as a secret from consumers for 20 years:

v1: echo “%1 is infected.”

Ask someone for v2! It’s even better. No FPs!

Conclusion

If The Perfect AntiVirus does not fail the test, the test is as silly as this example.

Don’t forget about v2.