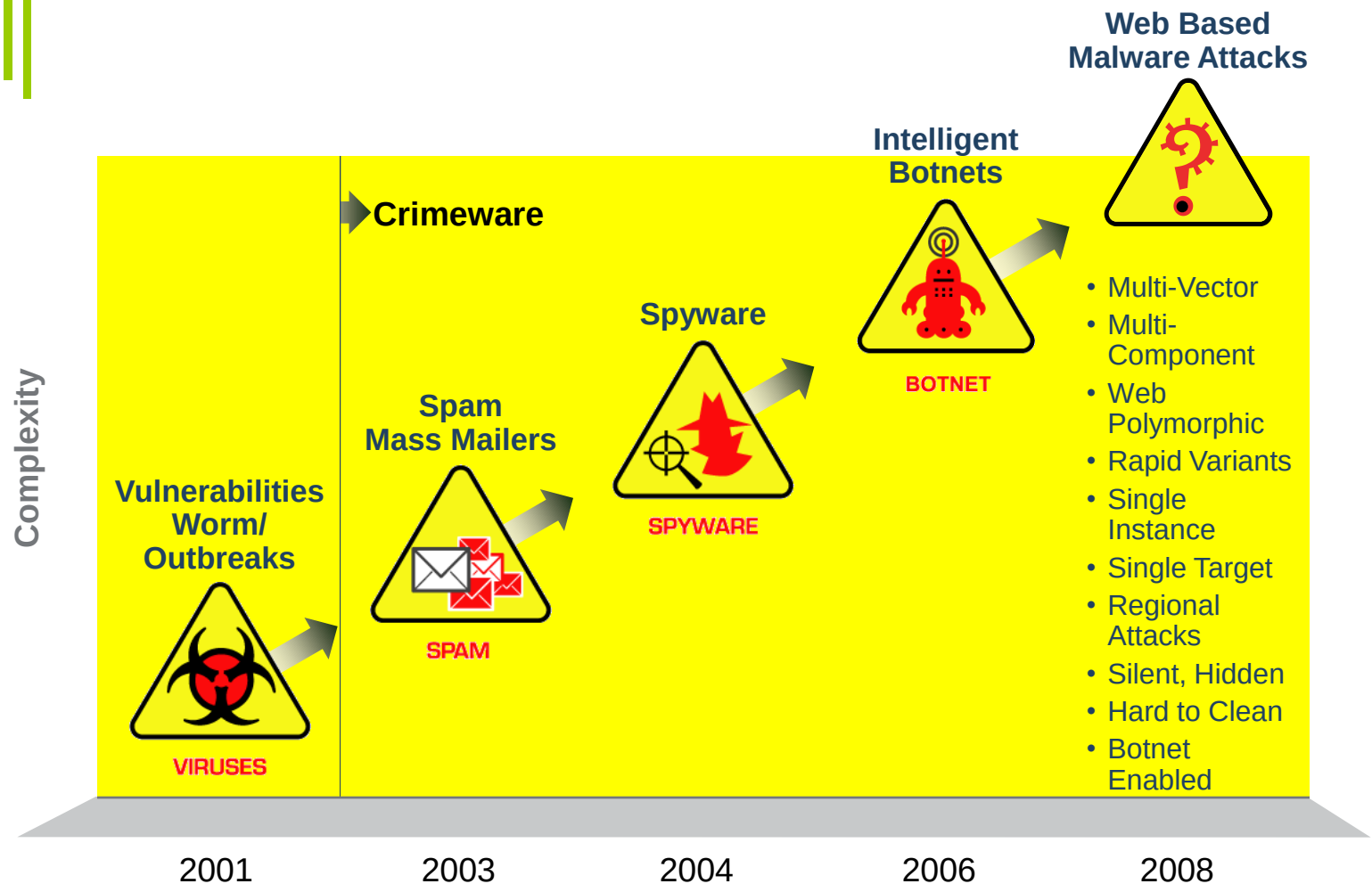
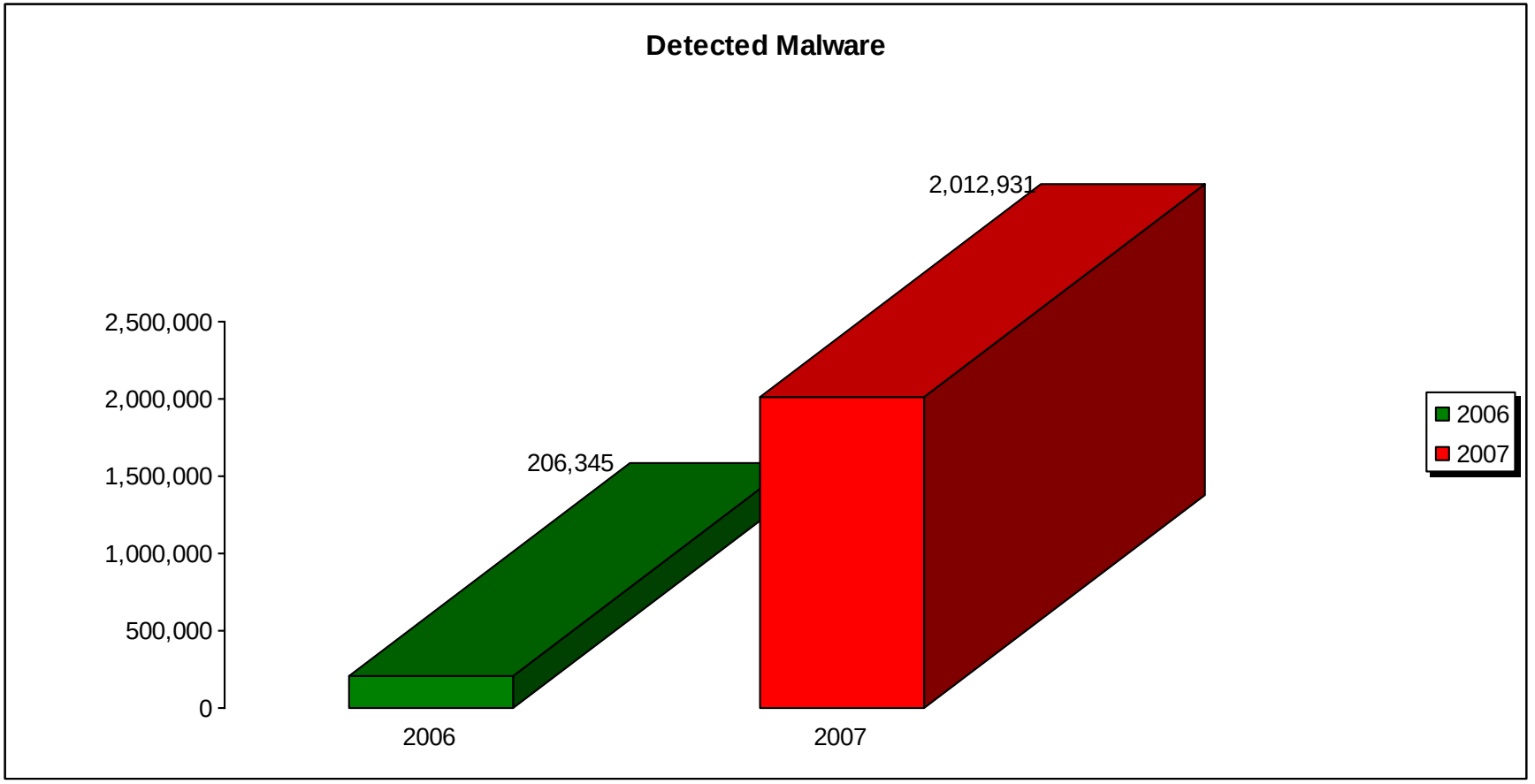
Herd Intelligence: true protection from targeted attacks

Ryan Sherstobitoff,
Chief Corporate Evangelist

PANDA SECURITY | *One step ahead.*


Web Based
Malware Attacks
Intelligent
Botnets
Crimeware
Spyware
Spam
Mass Mailers
Vulnerabilities
Worm/
Outbreaks
BOTNET
SPYWARE
SPAM
VIRUSES
Complexity
• Multi-Vector
• Multi-Component
• Web Polymorphic
• Rapid Variants
• Single Instance
• Single Target
• Regional Attacks
• Silent, Hidden
• Hard to Clean
• Botnet Enabled
2001
2003
2004
2006
2008

Growth of new threats



PandaLabs Research Study

ARE YOU REALLY PROTECTED?

Corporate Research Study

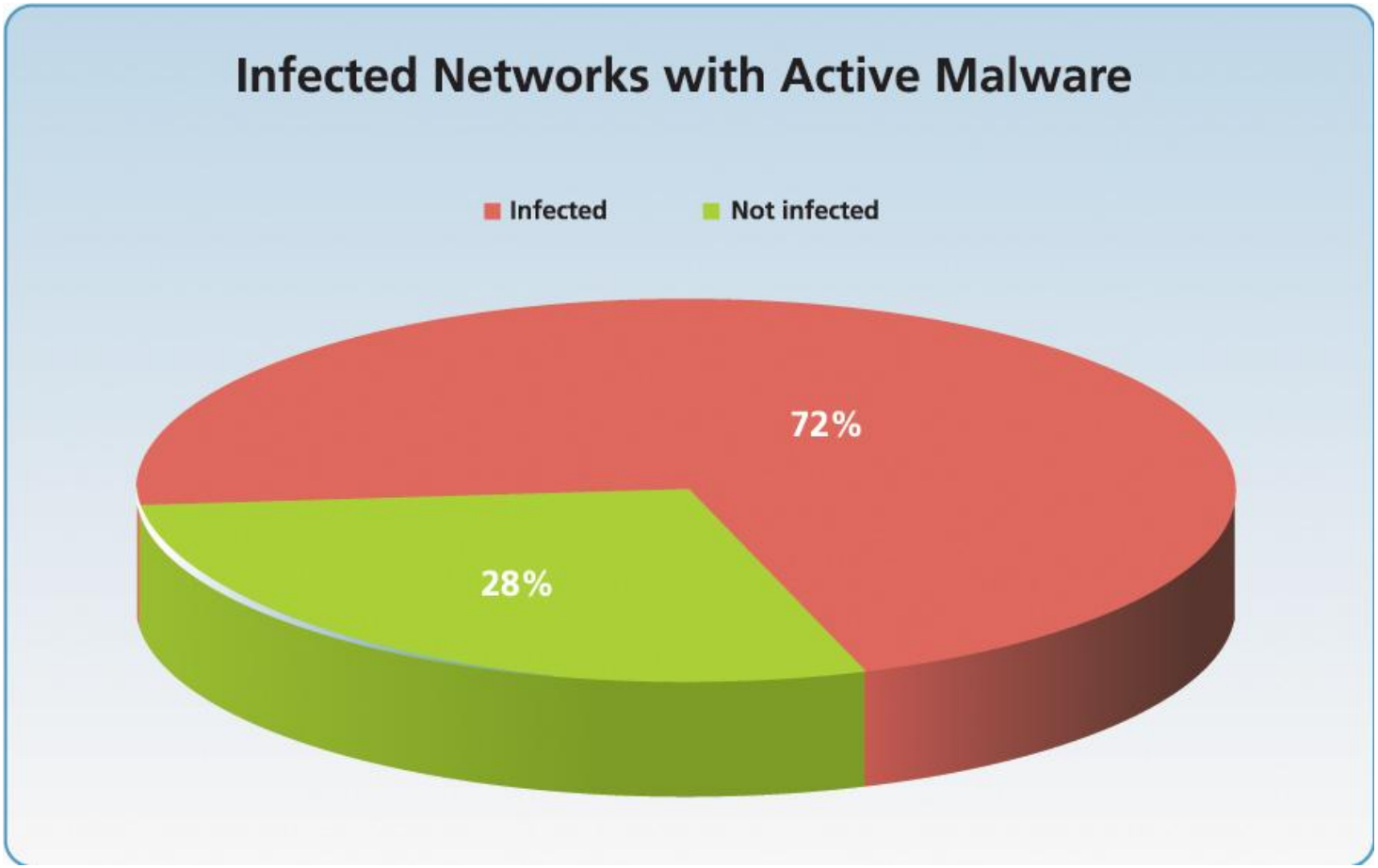
Study Facts and Guidelines

- **1209 companies from around the world took part in the corporate study. Their workstations were scanned using an audit service.**
- **Scanning utilized Herd Intelligence, a comprehensive hosted threat database**
- **The audit service tests active memory processes and objects, the installed protection and the protection status (enabled/disabled, up-to-date/outdated).**

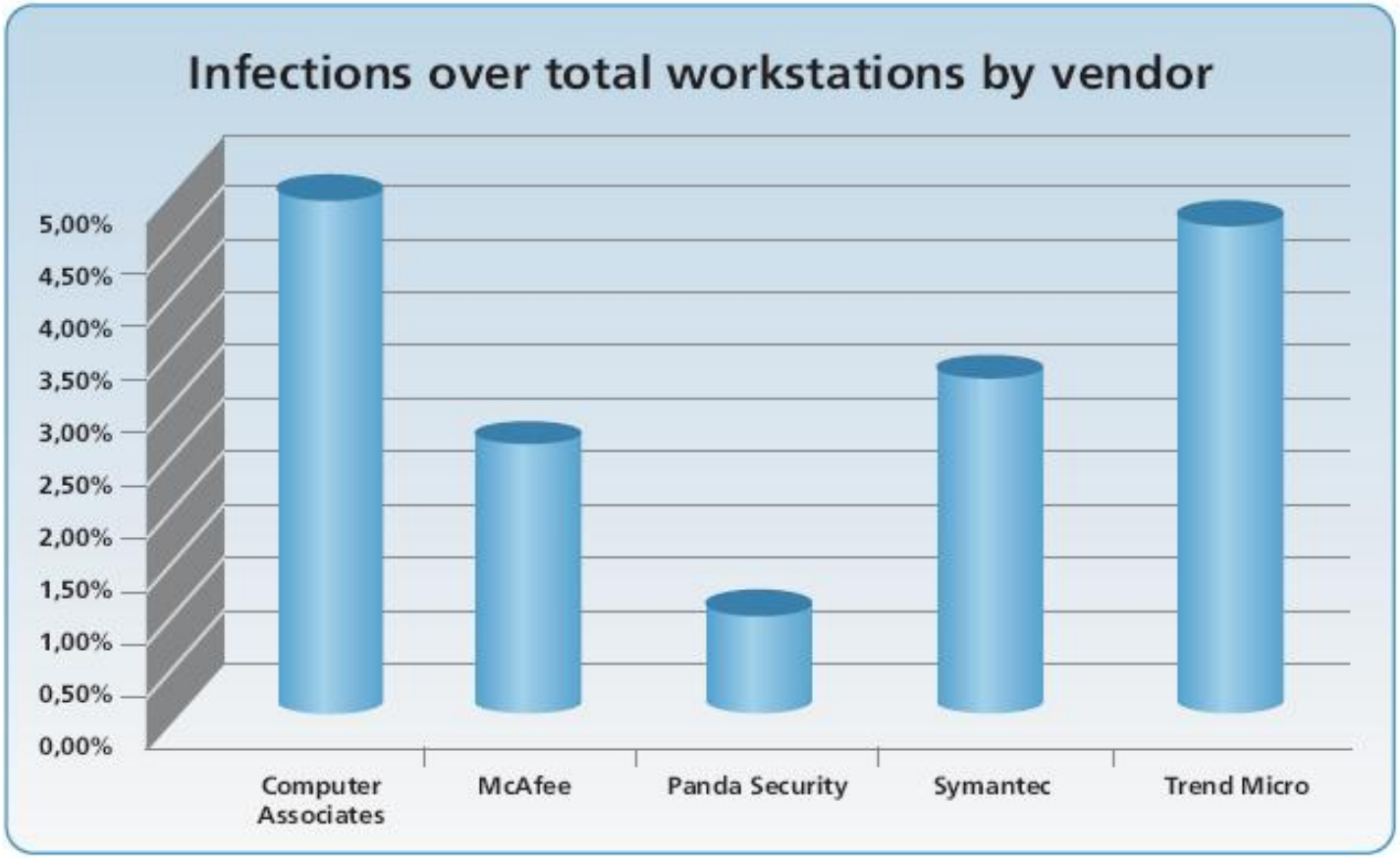
Corporate Research Study

- **The AV Vendor installed was deduced from Windows Security Center. In total, more than 40 separate solutions were recorded.**
- **Users that scanned their PCs several times were only counted once. Only the results of the first scan were taken into account.**
- **An endpoint was considered infected if we found malware running in memory.**
- **Latent malware (e.g. Trojans on the hard disk but not running), tracking cookies, jokes, etc. were not rated as infections.**

Research Results



Research Results

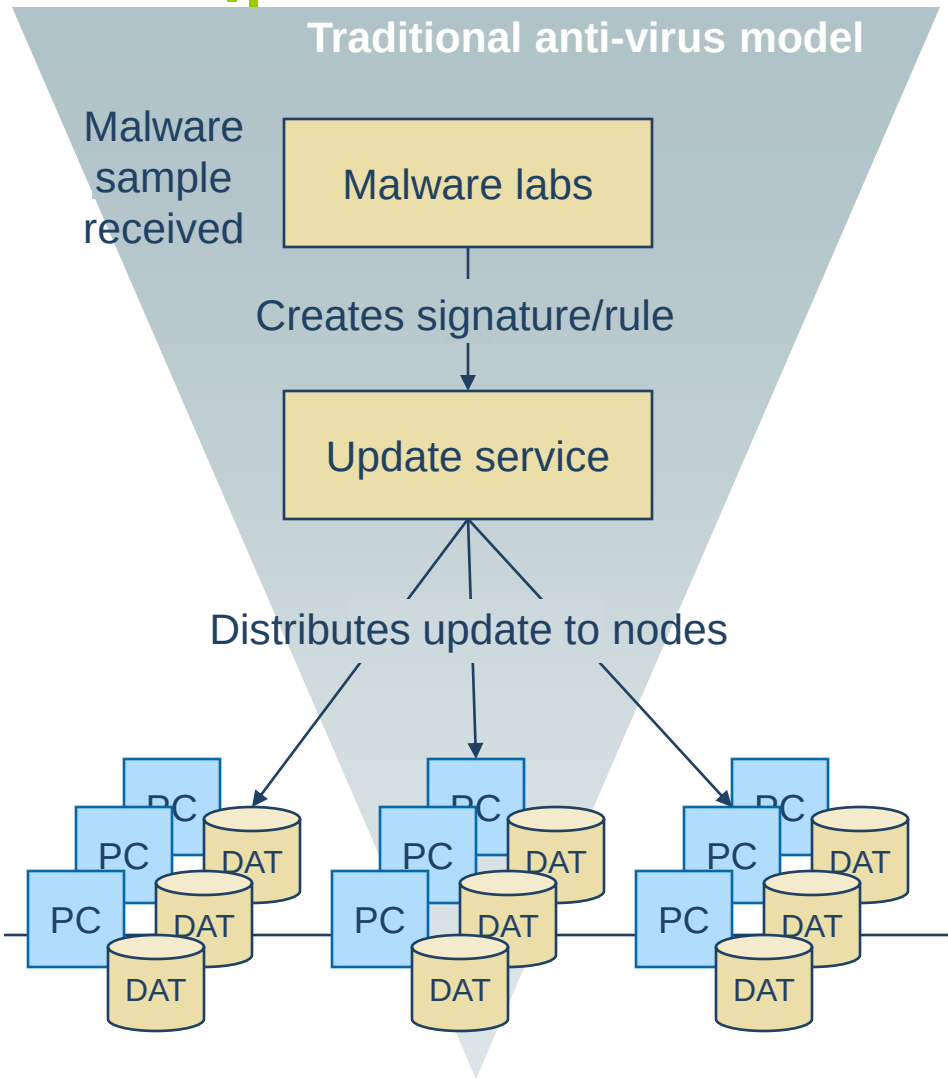


Why are 72% of Networks Infected?

How the bad guys are getting in with malware

- Silent Epidemics
- Financially Motivated
- Saturation of AV labs
- Targeted Attacks against the financial market
- Quality Control – testing against vendor’s signatures
- Virtual machine detection

A failing model

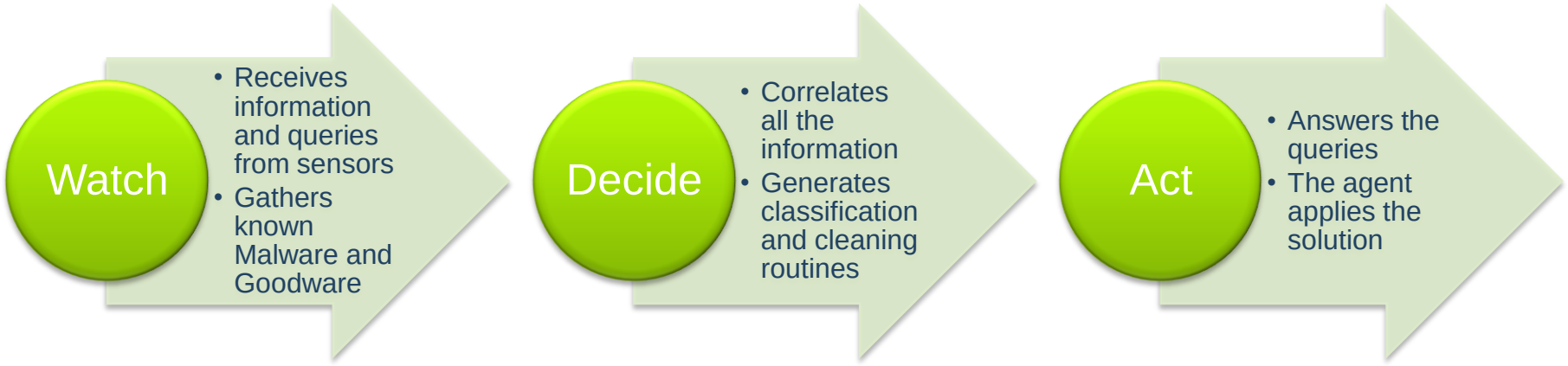


Weaknesses

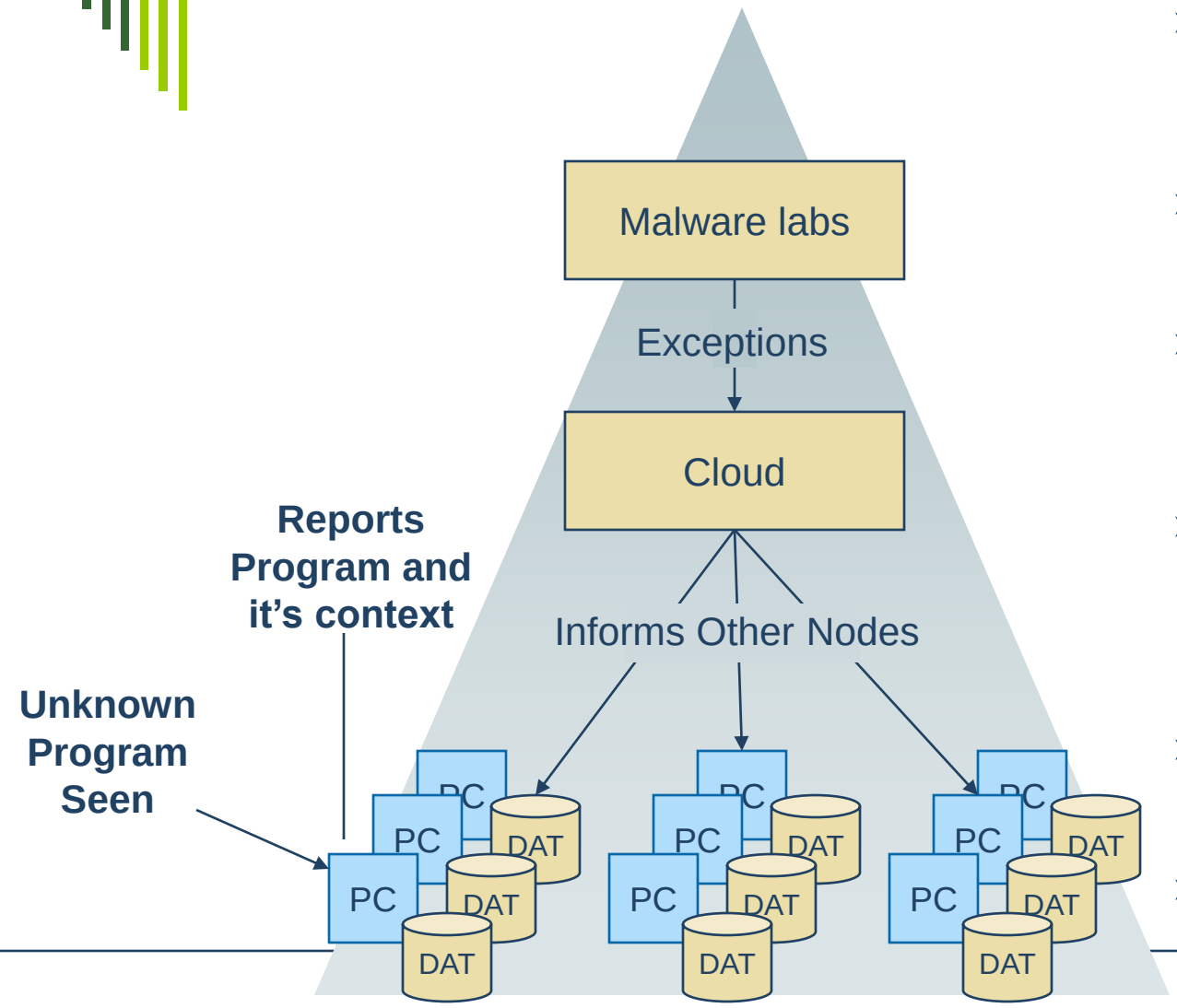
- No global threat detection/Intelligence
- No proactive protection (no required signature)
- AV Labs can not keep pace with signature creation requirements
- AV Labs must make compromises resulting in detection for less then 300,000 threats
- No automated signature creation
- Weeks to deliver new signatures
- Weak behavior blocking
- Weak heuristics identification

A new direction

Herd Intelligence



Herd Intelligence



Strengths

- Global threat detection
- Automated Signature creation-2 hours to distribution
- Proactive protection (no signature required)
- Automated malware analysis and automatic remediation
- Built on a SASS model with unlimited capabilities for storage, processing and delivery of knowledge
- Currently detects over 3 million threats
- Benefits from knowledge obtained in the community

Unmatched Security Data Processing

"It is a matter of survival for AV vendors, who increasingly are looking for ways to reinvent themselves as their product struggle to thwart new type of infections.

***Cloud-based, collective intelligence services are the next big thing for anti-malware**.*

I expect that every AV vendor will need to embrace an approach like this if they expect to survive"

Yankee Group

Cs monitored

illion malware samples

million programs analyzed

million correlations performed

ion records in our database

94,4% of all the detected malware in 2007 comes from Herd Intelligence

A new but necessary layer of defense

- Global visibility into the threat landscape reducing reaction time.
- On demand audits of virtualized networks.
- Locates unnoticed infection points that currently slip through existing defenses.
- Real-time protection against targeted attacks.