Symantec Endpoint Protection 12

Hundreds of Millions of New Pieces of Malware Mean You Have to Do Things Differently

Graham Ahearne, Marcus Brownell

Product Management

Agenda

1. Challenges
2. How Symantec Endpoint Protection can help
3. Questions & Answers

Challenges

Threat Landscape
Key Trends

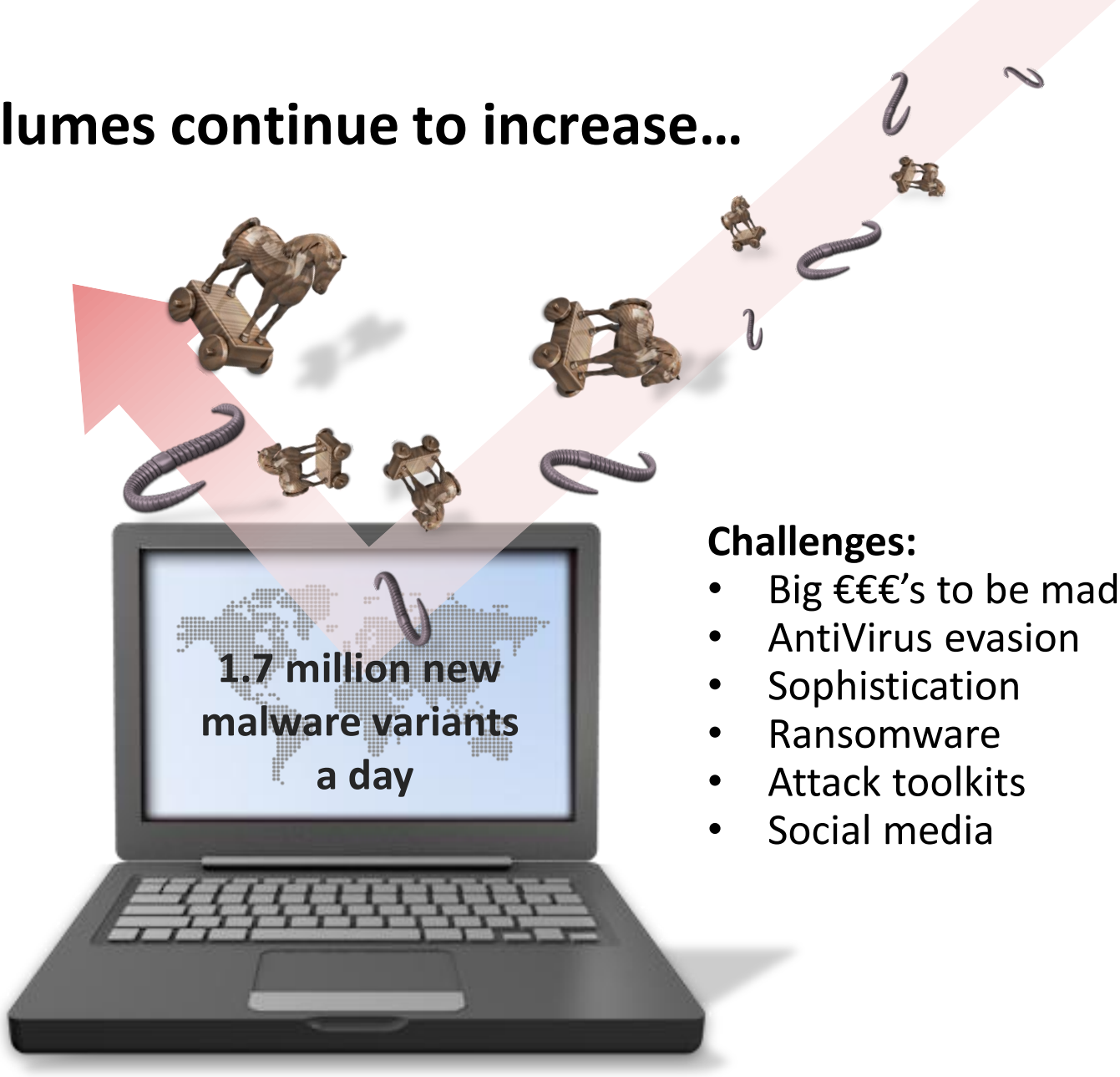
Malware Attacks 81% ↑

Targeted Attacks Expand

Data Breaches on Rise

Mobile Threats Expose All

Malware volumes continue to increase…

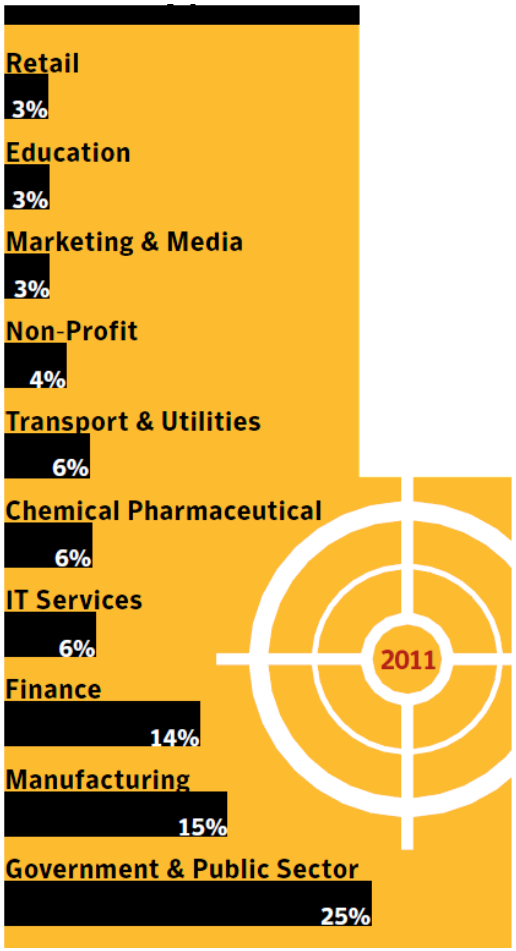


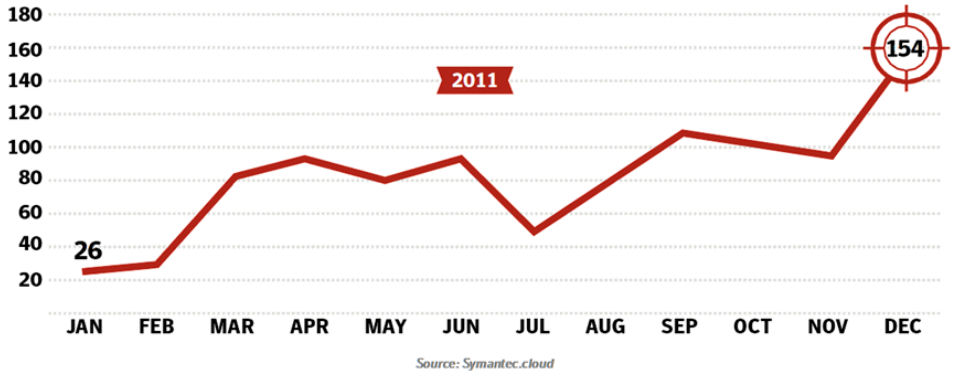
Challenges:

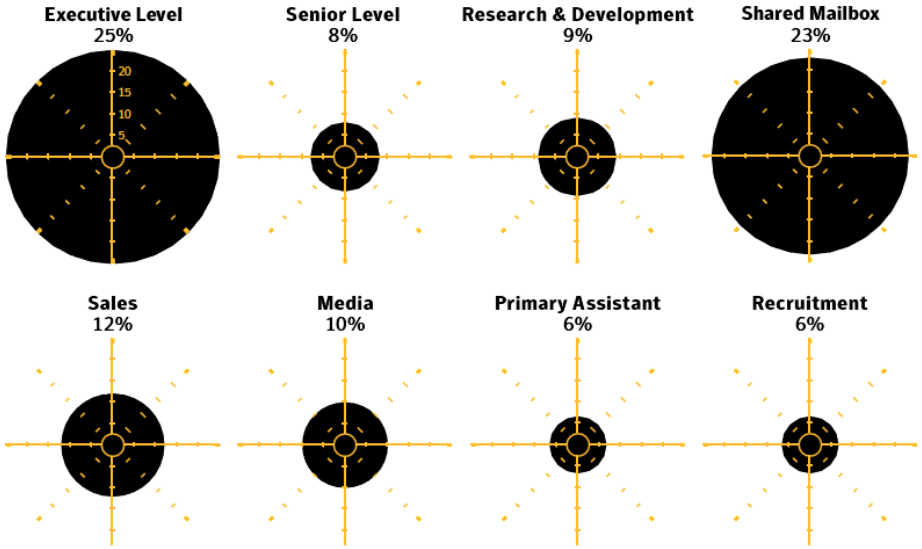
- Big €€€'s to be made
- AntiVirus evasion
- Sophistication
- Ransomware
- Attack toolkits
- Social media

Targeted attacks impact all

…& are on the increase







Data is the target, malware provides the means

Verizon Data Breach Report 2012: "**How does a breach occur?**"

69%

Of breaches involved malware
(+20% YoY)

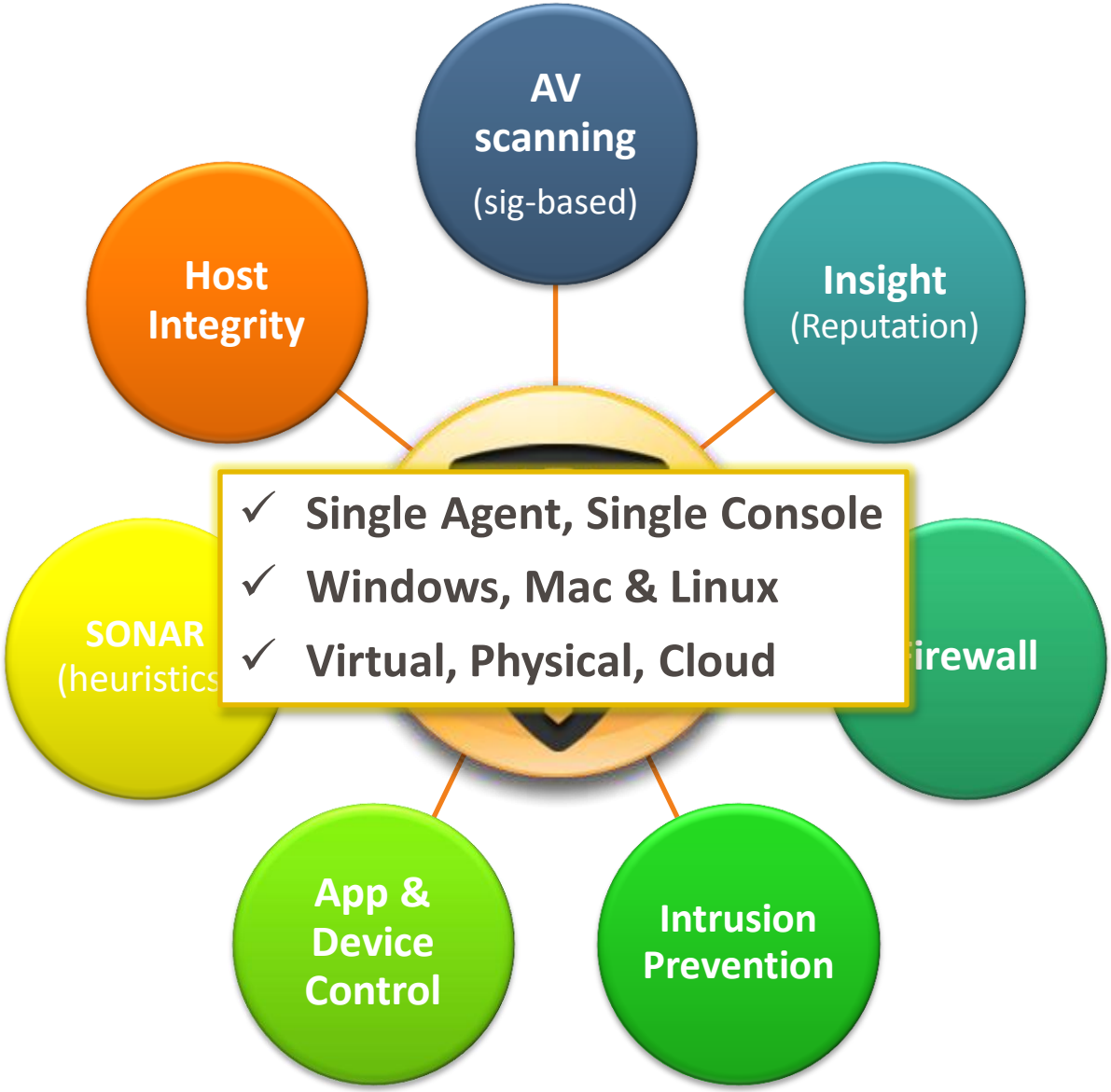
99%

Of record loss involved malware
(+15% YoY)

Not all endpoints are equal

Desktops/Laptops	Servers	Virtualisation	Mobile
			
▪ Large scale attack surface ▪ Performance-sensitive users ▪ Roaming frequently	▪ Availability and performance ▪ High value data ▪ Compliance ▪ Insider risk	▪ Density and IOPS ▪ High target value ▪ VM sprawl ▪ New vulnerabilities	▪ Fast proliferation ▪ Sensitive Data ▪ High risk of theft/loss

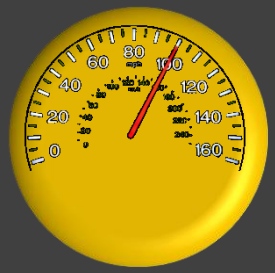
How Symantec Endpoint Protection can help


AV scanning
(sig-based)
Host Integrity
Insight
(Reputation)
✓ Single Agent, Single Console
✓ Windows, Mac & Linux
✓ Virtual, Physical, Cloud
SONAR
(heuristics
irewall
App & Device Control
Intrusion Prevention

Symantec Endpoint Protection 12 – Focus Areas

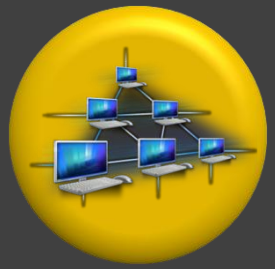
Unrivaled Security

- Reputation-based, signature-less, zero day protection



Blazing Performance

- Up to 70% reduction in scan overhead
- Smarter Updates



Built for Virtual Environments

- Optimized for virtual
- Higher VM densities
- vShield integration

Symantec Endpoint Protection 12 – Proven

8.5mil
Endpoints

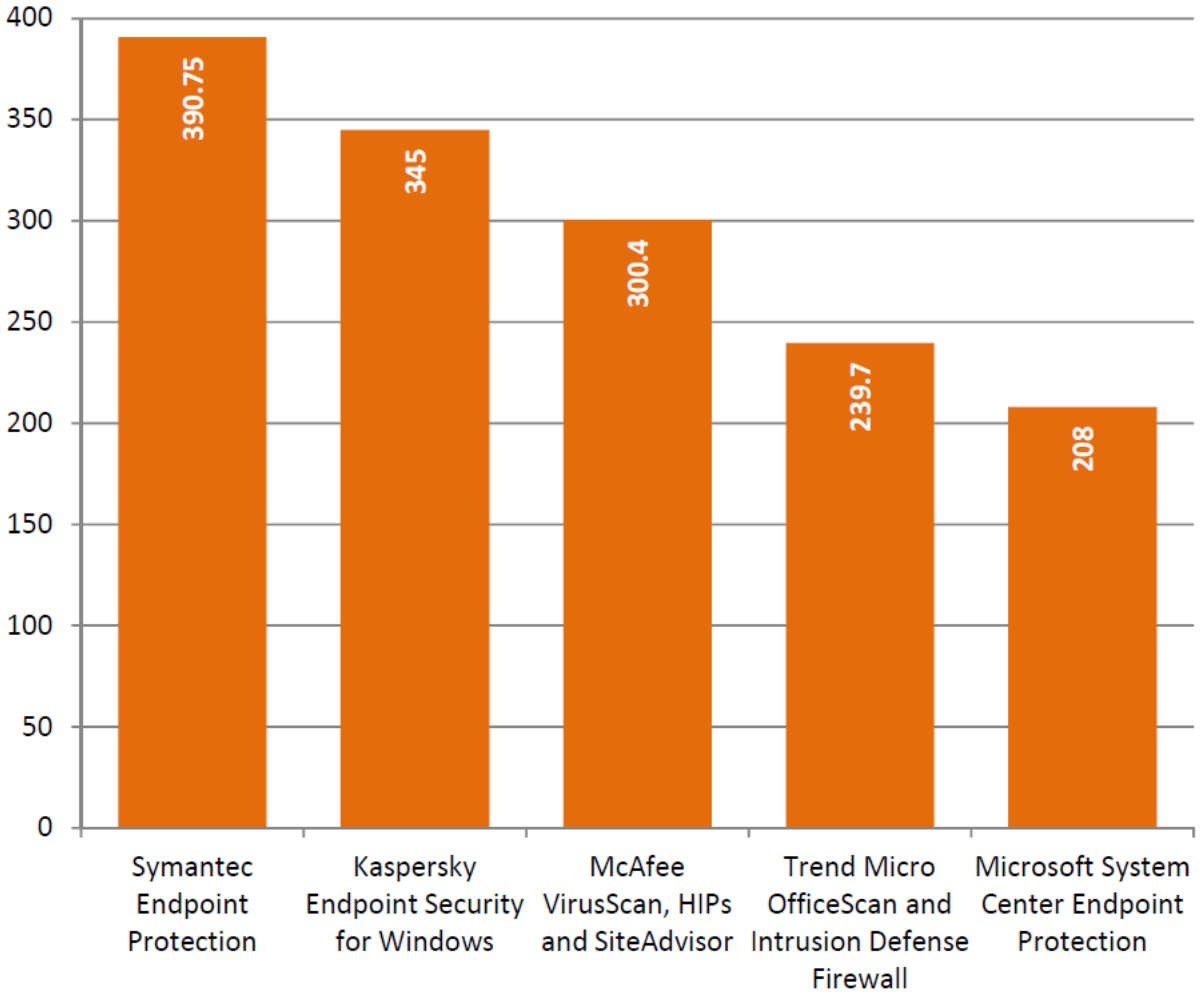
#1
Protection Performance

0
Hotfixes

#1
Gartner MQ Market Share

Dennis Labs: Endpoint Protection effectiveness test

Published October 2012



Symantec only vendor to receive:

DENNIS AAA TECHNOLOGY LABS

- This is a purely neutral, non-vendor sponsored test.
- Score takes into account number of false positives.

Symantec Endpoint Protection 12
Customer feedback on real world experience

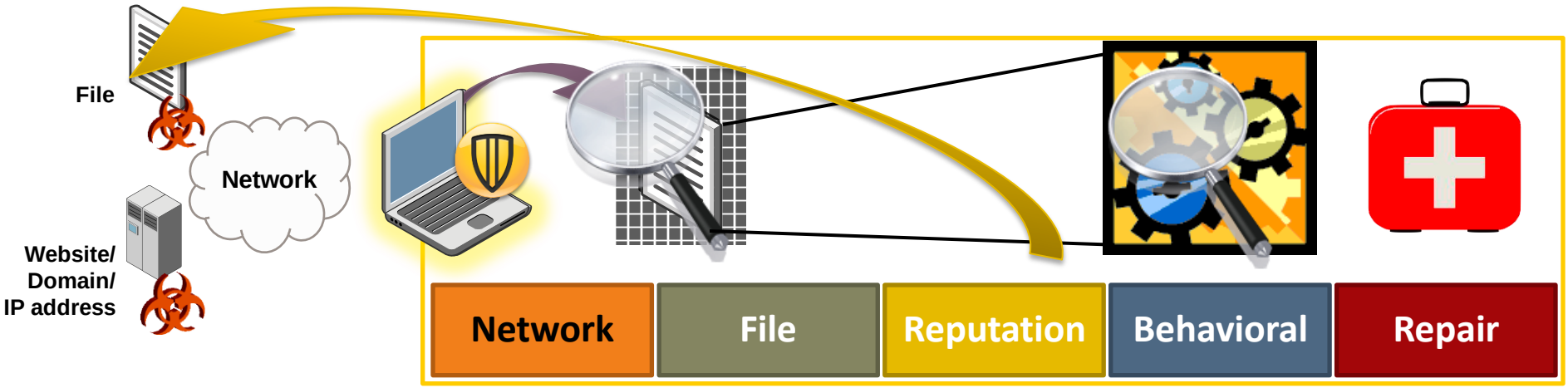
Computacenter

- 11,000 users worldwide
- Upgrade from SEP 11.x
- *"The SONAR 3 and Insight functionality in Endpoint Protection 12.1 is flawless. Our consultants' laptops are starting much more quickly and running faster."*
  - Martin Rutkowski, Computacenter

Ford Motor Co.

- 180,000 nodes deployed globally across 402 sites.
- Moved from competitor to SEP 12.1 due to performance and protection effectiveness issues.
- Major end-user satisfaction increase due to performance gains during scans, boot time and everyday usability.

Multiple complimentary protection layers



1 Network-based Protection

Stops malware as it travels over the network and tries to take up residence on a system

- Protocol aware IPS
- Browser Protection
- Patch mitigation

2 File-based Protection

Detects and cleans malware that has already taken up residence on a system

- Auto Protect
- Heuristics (Malheur)

3 Reputation-based Protection

Establishes information about entities e.g. websites, files, IP addresses

- Domain Reputation
- File Reputation (INSIGHT)

4 Behavioral-based Protection

Looks at processes as they execute and scans for malicious behavior

- Heuristics (SONAR)
- Runs in real time

5 Remediation Tools

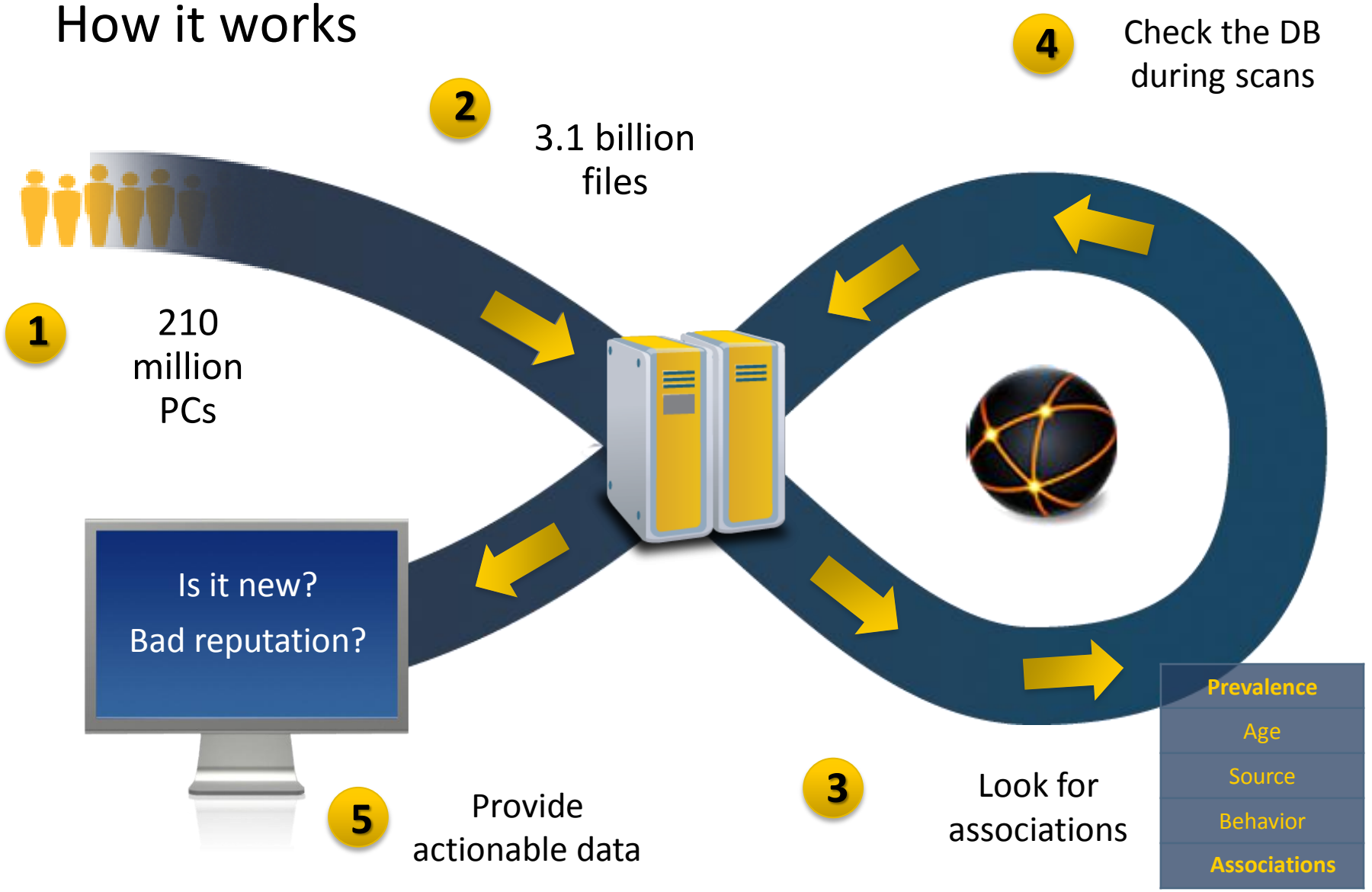
Aggressive tools for hard to remove infections

- Boot to a clean OS
- Power Eraser

Automatic “hands-off” protection for exploits targeting 3rd party software

Insight: True reputation based protection

How it works



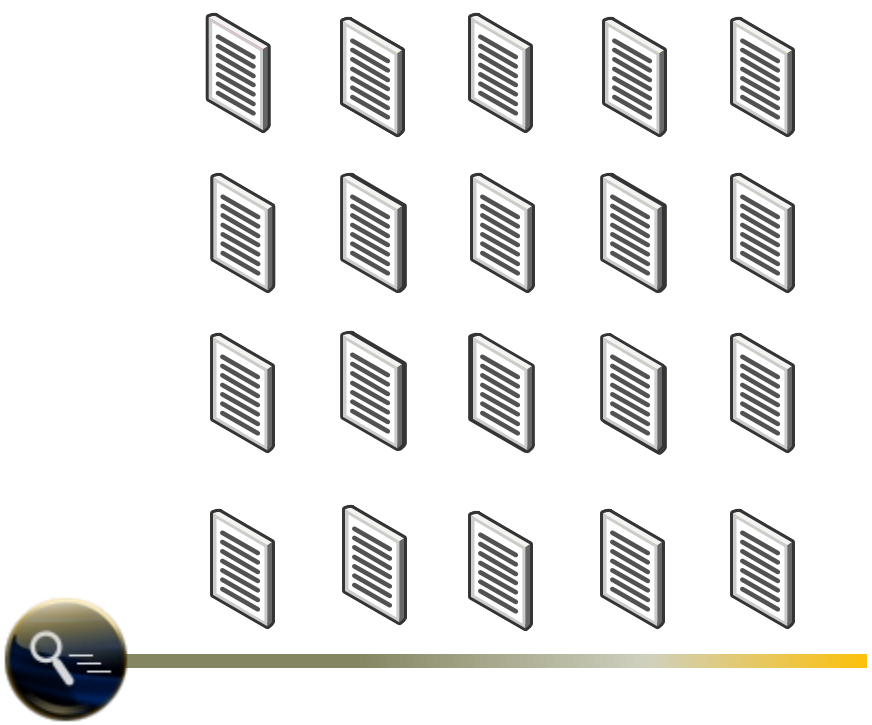
SONAR: Endpoint behavior-based heuristics
A day in the life of… (19th March 2012)

- Detected **106,829** files on **55,841** unique machines
- Which competitors had detection for these malicious samples?
  - Kaspersky – 24.3%
  - Microsoft – 16.7%
  - McAfee – 1.7%
  - Trend – 0.00126%
- Enabled as **block by default**, extremely low false positive rate
- Blocked zero day attacks such as Aurora, Stuxnet and Elderwood

Monitors close to 1400 behaviours (bad & good), in real time

Why Scan Everything, when you can scan a Fraction?

Typical Approach



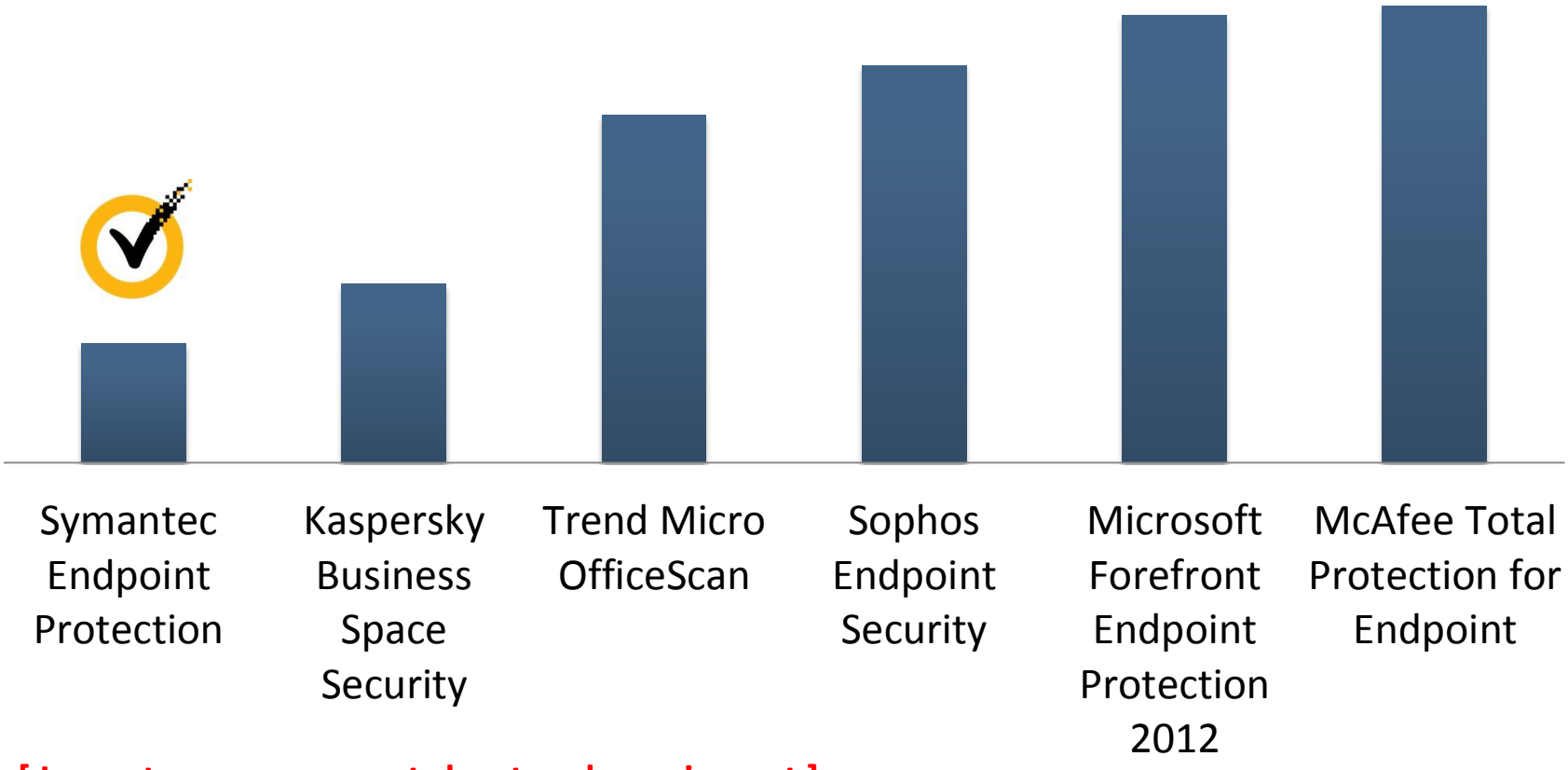
Scans *every* file

SEP 12.1

Only scans new & untrusted files

Best-in-class performance, for user productivity

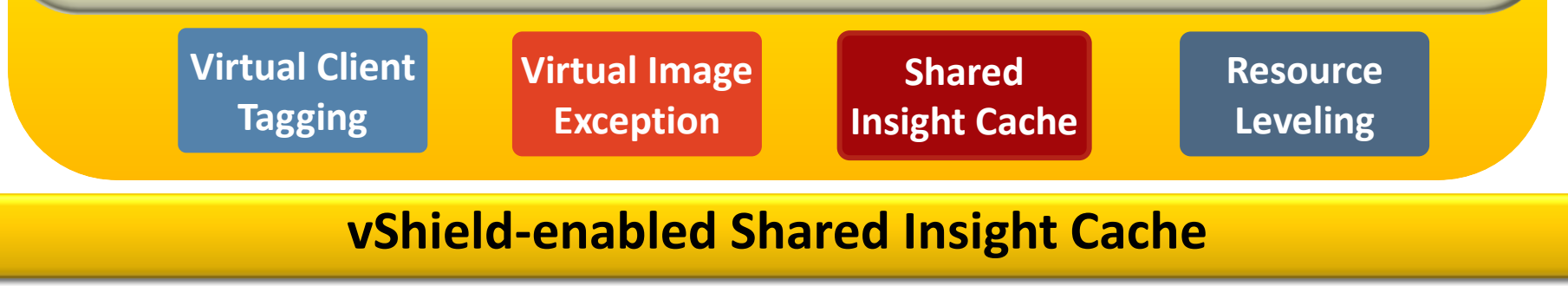
Passmark Enterprise Endpoint Protection Benchmark



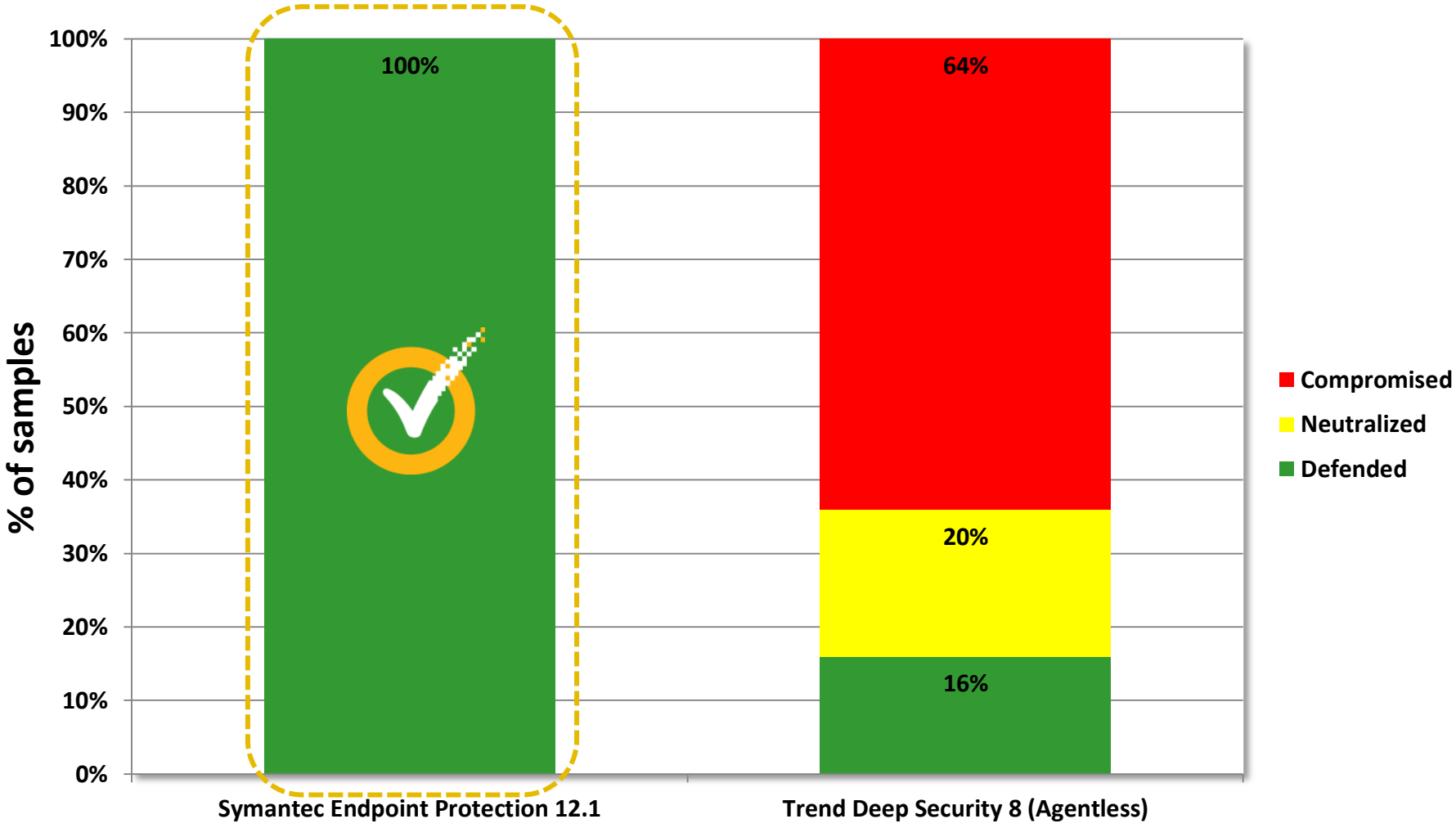
[Lowest score represents least end user impact]

Optimised Performance in Virtual Environments
Without sacrificing protection…

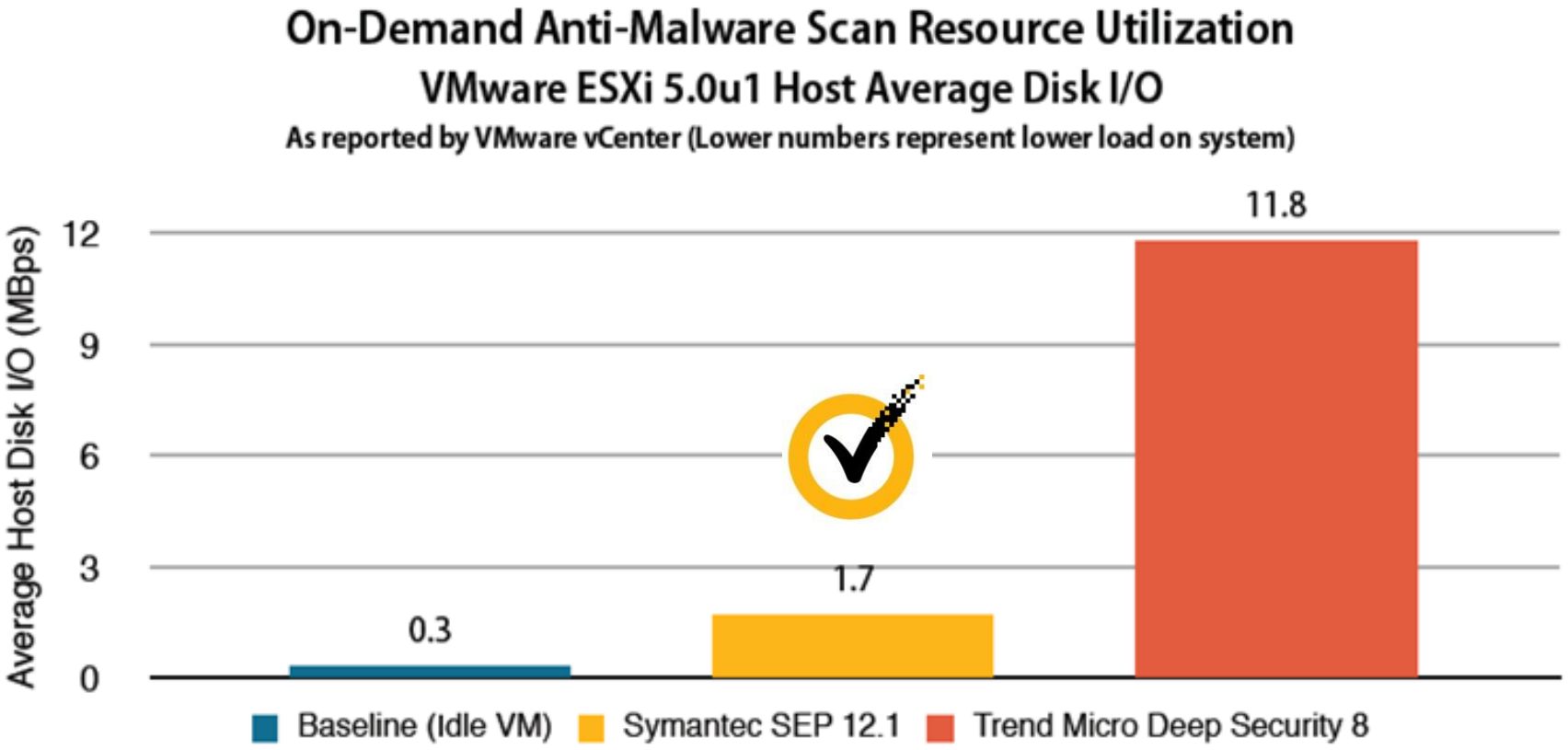
- **Eliminate** scan activity with ***Insight*** and ***Virtual Image Exception***
- **De-duplicate** remaining scan activity with ***Shared Insight Cache***
- **Smooth out** remaining scan and update activity with ***Resource Leveling***



SEP 12 vs. Trend Micro Deep Security 8
Protection Effectiveness



SEP 12 vs. Trend Micro Deep Security 8
Virtual Machine Performance



Symantec Endpoint Protection 12.1.2 (RU2)
What's New

Platform Support
- Windows 8, Windows Server 2012
- VMware vShield Integration
- Mac OSX Mountain Lion

Enhanced Management
- Group Update Provider Roaming
- Further optimisations for VDI
- Remote Monitoring & Mgmt

Enhanced Protection
- Attacks across encrypted channels
- Enhanced IP/Domain Reputation
- Social media based attacks

Lower total cost of ownership
- Centrally recover orphaned clients
- Updated self diagnostics & help tool
- Expanded software for auto-replace

Windows 8
Primary threat vectors are still a problem

- Drive-by Downloads/Web Attacks
- Social Engineering
- Bots and Botnets
- Misleading Applications
- Social Media Attacks
- Malicious URLs
- 0-day Malware
- Network Worms
- USB Key Infections
- Crypted and Packed Malware
- Malicious PDFs and Office Documents
- Unpatched Vulnerabilities

Windows 8
Compatibility & Windows Style Support

- **Toaster Notifications**
  - Only approved way to deliver critical notifications from desktop apps to Windows Style is via “toaster” notifications
  - SEP will support toaster notification
- **Windows Style App Remediation**
- **Early Launch Anti Malware (ELAM)**
  - Driver support

Wrap-up

Unmatched Protection	• Leading threat intel and protection technologies (such as Insight) keep you ahead of the curve
Keep TCO down	• Designed to provide out of the box value and integration with minimum config
From brand you can trust	• #1 Security Software company • Protect 99% of fortune 500

Related Sessions of Interest

Time	Topic	Location
Next	IS B04 SEP 12 Customer Panel: Experiences of migration to SEP 12	This room
Wednesday 9:00-10:00	IS B10 Securing your virtual data centres: the future of endpoint and server security	114
Wednesday 10:30-11:30	IS B08 The anatomy of modern attacks	127/128
Wednesday 17:15-18:15	IS B14 Are you getting the Most From Symantec Protection Suite	TBC
Thursday 9:00-10:00	IS B09 SONAR, Insight, Skeptic and GIN – The Symantec secret sauce	TBC

Thank you!

Graham_Ahearne@symantec.com

Marcus_Brownell@symantec.com