Cyber Threats and SMB's What Your Business Can Do to Be Informed and Protected

10 Fallacies about Endpoint Security

Hosted by Kaspersky Lab and Waytek

Intro and background

- **Brian McDonnell, CEO**
  - 29 years in the IT industry
  - Built and ran multiple IT and security businesses
  - Most recently, built a security and compliance software company call Rippletech – ultimately acquired by Intel
  - Acquired Waytek in 2009
  - My philosophy is to align ourselves with our client

waytek
...a step ahead

Waytek

- We are an IT company with a national and local presence.
- Locally, we focus on Managed or Remote IT Services for SMB's in the area.
- We build our business by building relationships with customers and providing a holistic approach to their IT security needs.
- In addition, we try to educate our customers and keep them up to date through social media, our website and blogs, events like these, and our newsletter. (Here's an example of our newsletter.)
- As you'll hear from the presentation, it's not enough to just protect. The security experts at Waytek provide protection, detection AND response.

waytek
...a step ahead

Multi layer security monitoring

Performace

Network Health

Patching and alerts

Client Information

Contact Person	
IT Manager	
Servers Managed	6
Workstations Managed	1
Total Systems Managed	7

System Activity Last 30 Days

Audits Completed	203

Ticket Status

Tickets Created Last 30 Days	6
Total Tickets Past Due	1
Tickets Closed Last 30 Days	0
Total Open Tickets	6

Anti-Virus

Summary Statistics

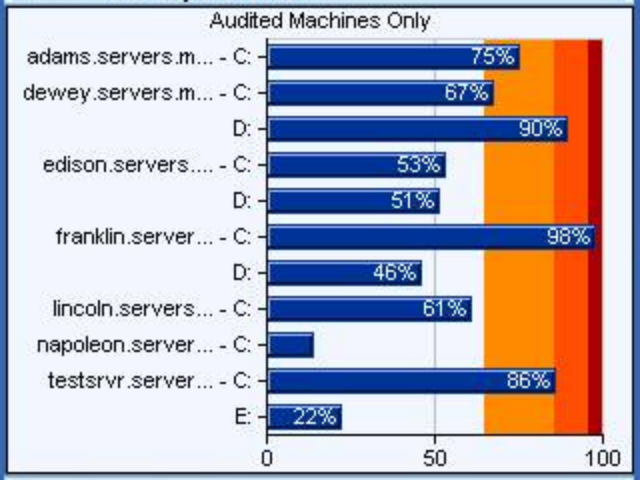
Machine Installation Ratio	0/7

Anti-Malware

Summary Statistics

Workstation Installation Ratio	0/1
Server Installation Count	0

Disk Space Used



Server Uptime

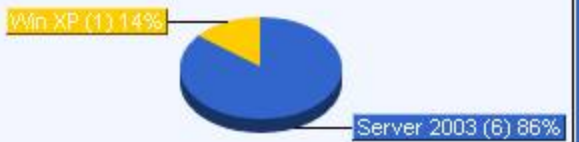
Machine ID	% Uptime
adams.servers.main-office.admi...	94.5%

Network Health Score

Patch Score	100%	* 1/7
OS Score	100%	* 1/7
Disk Score	70%	* 1/7
Ticket Score	89%	* 1/7
Event Log Score	100%	* 1/7
Alarm Score	86%	* 1/7
Srv Uptime Score	100%	* 1/7
Wrk Uptime Score	N/A	* N/A

92%

Operating Systems



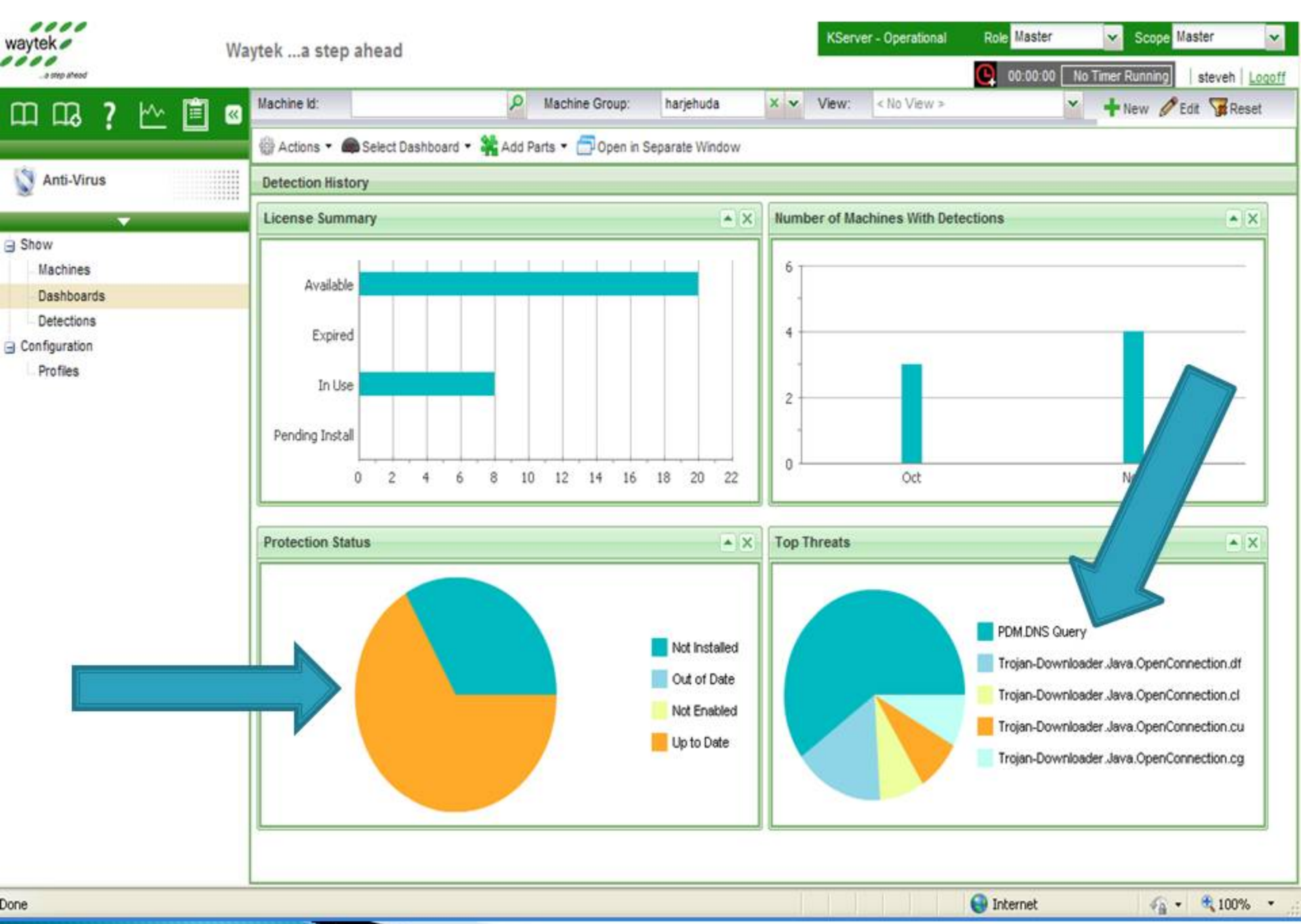
Patch Status

Patch Scans Completed	64
Patches Installed	5

Alarm Notifications

Alert	Agent Offline	84
Alert	Agent Online	46
Alert	New Patch	6
Agent Set	S critical.Exchange.Core.Service...	22
Agent Set	C normal.exchangeperformance.cou...	1
Agent Set	S ZC-EX1 - Exchange Basic Servic...	3
No SNMP Alarms Found		0
No System Check Alarms Found		0
No Log Parser Alarms Found		0

License Summary


waytek
Waytek ...a step ahead
KServer - Operational
Role Master
Scope Master
00:00:00 No Timer Running
steveh | Logoff
Machine Id:
Machine Group: harjehuda
View: < No View >
New Edit Reset
Actions Select Dashboard Add Parts Open in Separate Window
Anti-Virus
Show
Machines
Dashboards
Detections
Configuration
Profiles
Detection History
License Summary
Available
Expired
In Use
Pending Install
0 2 4 6 8 10 12 14 16 18 20 22
Number of Machines With Detections
6
4
2
0
Oct
Protection Status
Not Installed
Out of Date
Not Enabled
Up to Date
Top Threats
PDM.DNS Query
Trojan-Downloader.Java.OpenConnection.df
Trojan-Downloader.Java.OpenConnection.cl
Trojan-Downloader.Java.OpenConnection.cu
Trojan-Downloader.Java.OpenConnection.cg
Done
Internet
100%

Waytek

- At the heart of Waytek, we want to deliver the best service to our customers to make them feel more secure without worrying about the details of getting there.

- We really do want to make them feel that we are helping them be “a step ahead.”

Brian McDonnell
brianm@waytek.com
www.waytek.com
856 346 9310

waytek
...a step ahead

KASPERSKY lab

Be Ready for What's Next - 10 Fallacies about Endpoint Security

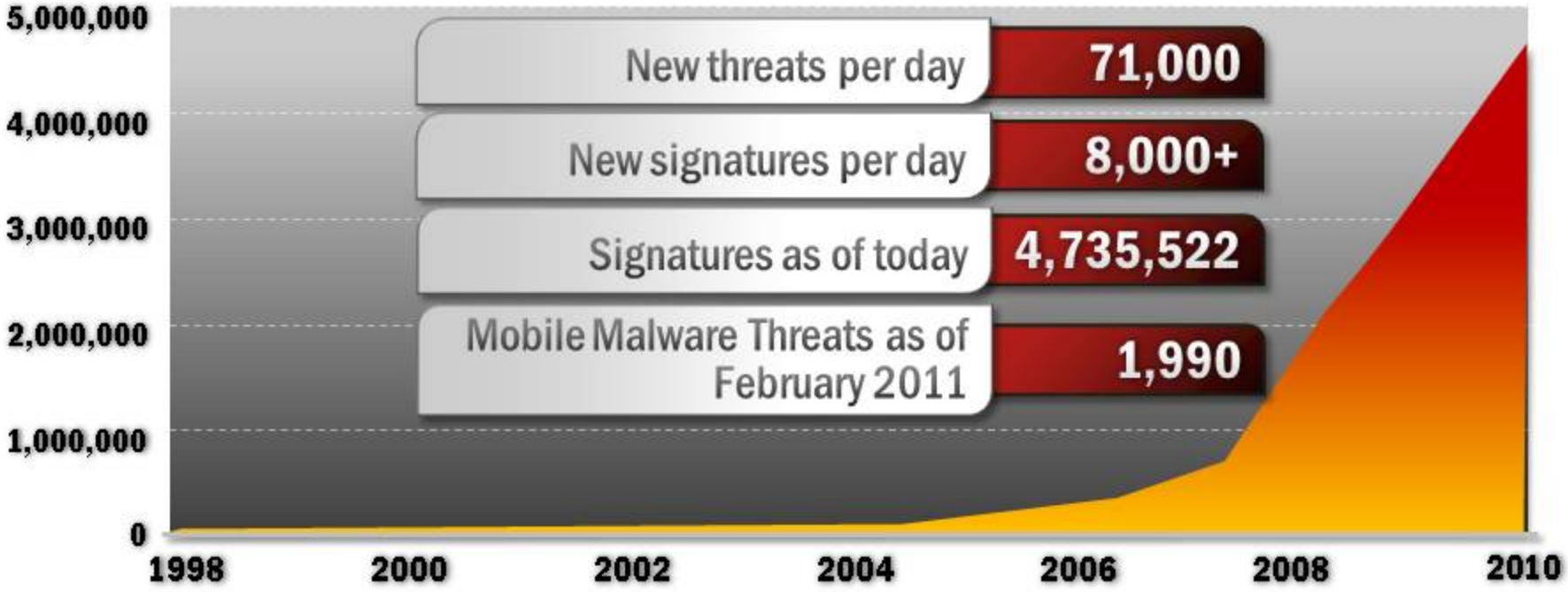
Ori Ammar, CISSP-ISSAP, CISA, CISM, CRISC
Systems Engineer
Kaspersky Lab

The Endpoint Is The Target

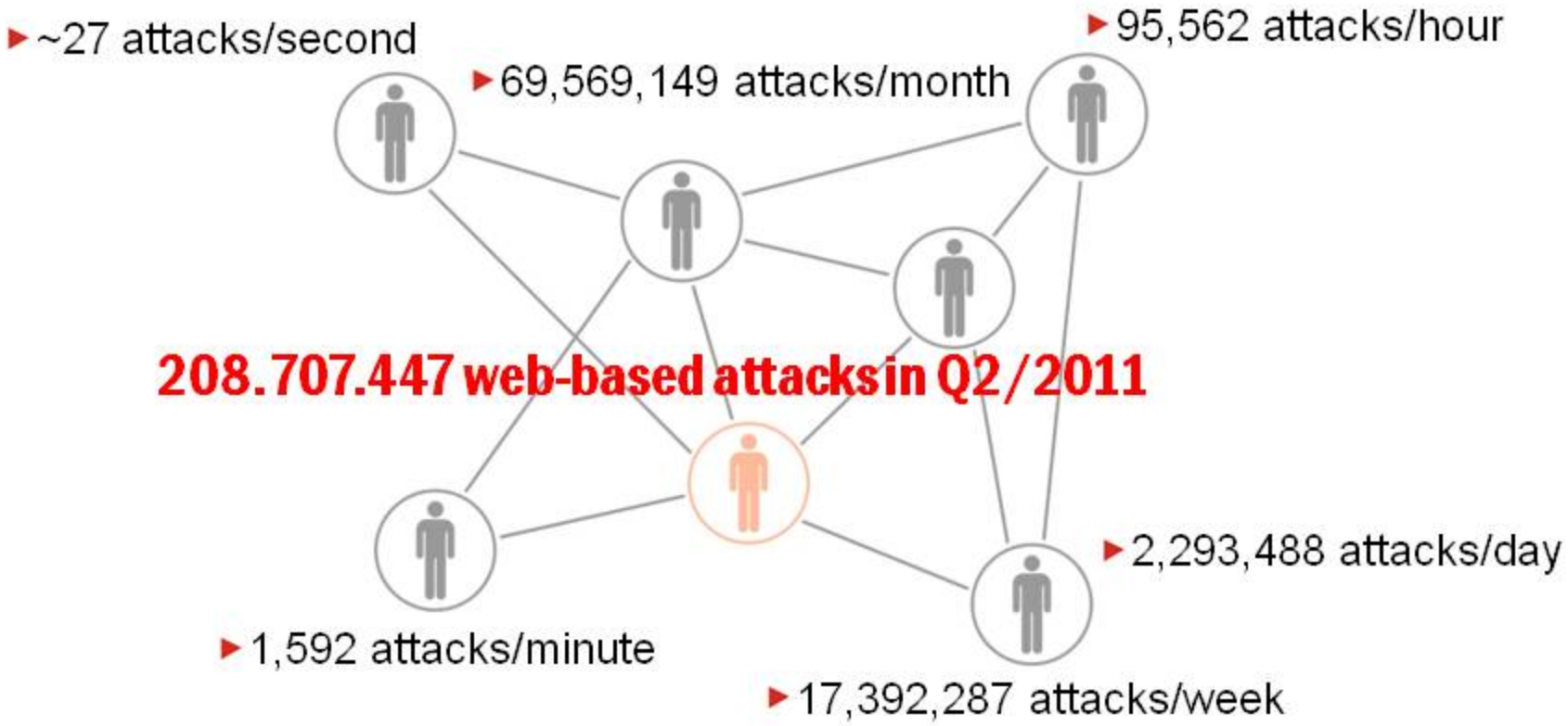
Malware On The Endpoint Is The Goal

Kaspersky's Global Perception

The Growing Malware Threat



Web-based attacks



Breaching the Most Secure

Computer Spies Breach Fighter-Jet Project

+ More | + Text -

billion Joint Strike
ever -- according to

ystem in recent months,
ere able to copy and
stems, officials say.

tween the U.S. and
The revelations follow a
S. electrical-distribution
es abroad.

-- or U.S. awareness of
ave escalated in the past
he former official briefed on
never been anything like
, adding that other military
s as well as private
ected. "It's everything that
going."

US Air Force

HACKING VICTIM: Spies are said to have stolen data on the F-35 Lightning II fighter. Here, the plane undergoes flight testing over Texas.

Many details couldn't be learned, including the specific identity of the attackers, and the scope of the damage to the U.S. defense program, either in financial or security terms. In addition, while the spies were able to

Air Traffic Control System Repeatedly Hacked

A security audit finds a total of 763 high-risk, 504 medium-risk, and 2,590 low-risk vulnerabilities, such as weak passwords and unprotected folders.

By Thomas Claburn
InformationWeek
May 7, 2009 06:16 PM

In the past four years, hackers have hobbled air traffic control systems in Alaska, seized control of Federal Aviation Administration network servers, and pilfered personal information from 48,000 current and former FAA employees, according to a newly released government report.

The report, "Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems," was published Wednesday by the Department of Transportation Office of the Inspector General.

It comes on the heels of a report last month in the *Wall Street Journal* that the Air Force's air traffic control system had been breached by hackers and amid congressional hearings featuring military and civilian officials testifying about the sorry state of U.S. cybersecurity.

IG: Air traffic con... cyberattack

By Kathleen Hickey

The Federal Aviation Admin... to cyberattacks via Web ap... new report released by the... General (OIG).

"In our opinion, unless effe... matter of when, not if, [air t... serious harm to [air traffic ... assistant inspector genera... the report.

Reps. John Mica (R-Fla.) a... "Review of Web Applicatio... Control Systems."

The satellite-based air traffic control system is heavily reliant on commercial software and IP-based technology. Among the auditors' conclusions:

1 Data Center Fixation

Assuming the data is in the data center

IDC research shows that desktops & laptops represent the most serious concern for Data Loss Prevention (DLP.)

2 Information Amnesia

Forgetting the value of data on mobile devices

2 Information Amnesia

Forgetting the value of data on mobile devices

3 Migration Myopia

Believing that company data never finds its way to home systems.

4 Device Delusion

Treating mobile devices as desktops

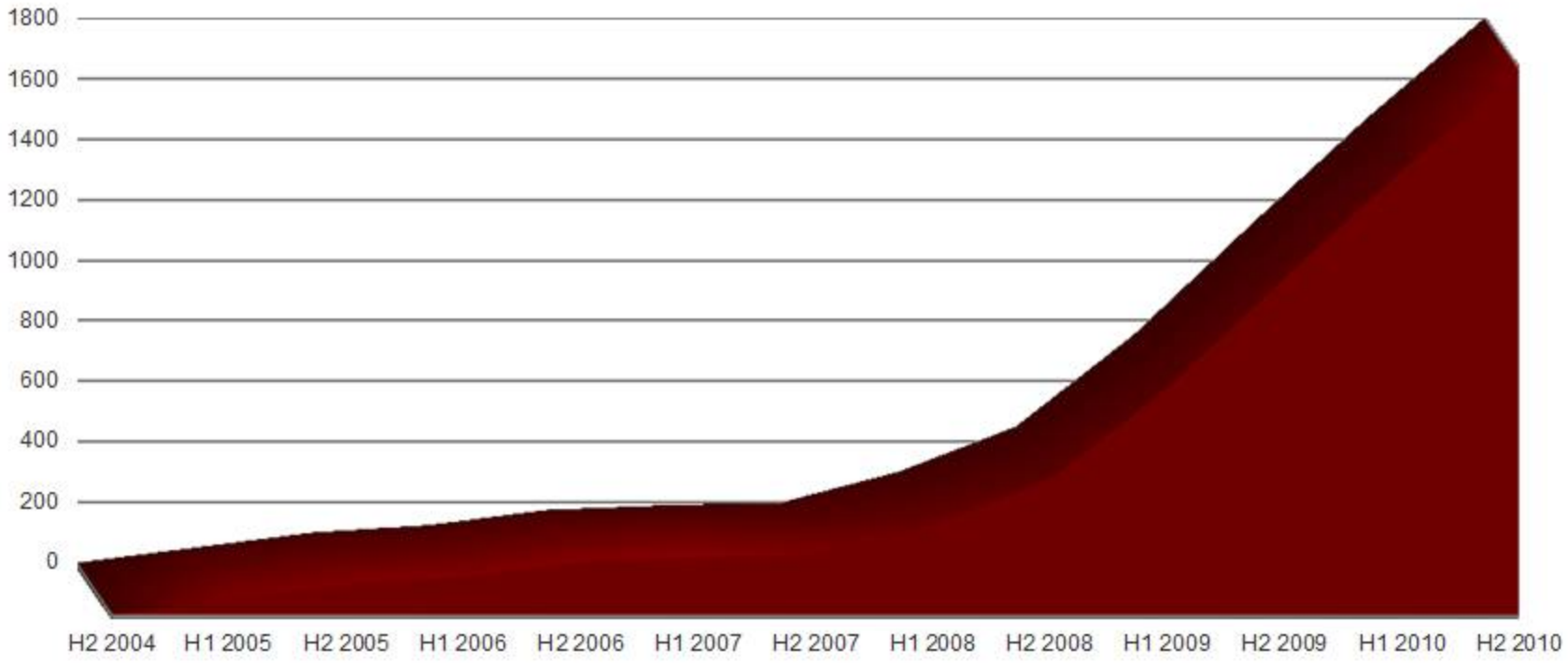
People are working – accessing the most up-to-date information, responding immediately to client contacts, and taking care of many more daily tasks – around the clock. .....this environment has created a new corporate vulnerability that is likely to be targeted by emerging threats.

– IDC

Mobile malware

Number of signatures

- Mobile threats are on the rise
- Total number of mobile malware signatures as of 26th September 2011: **4134**



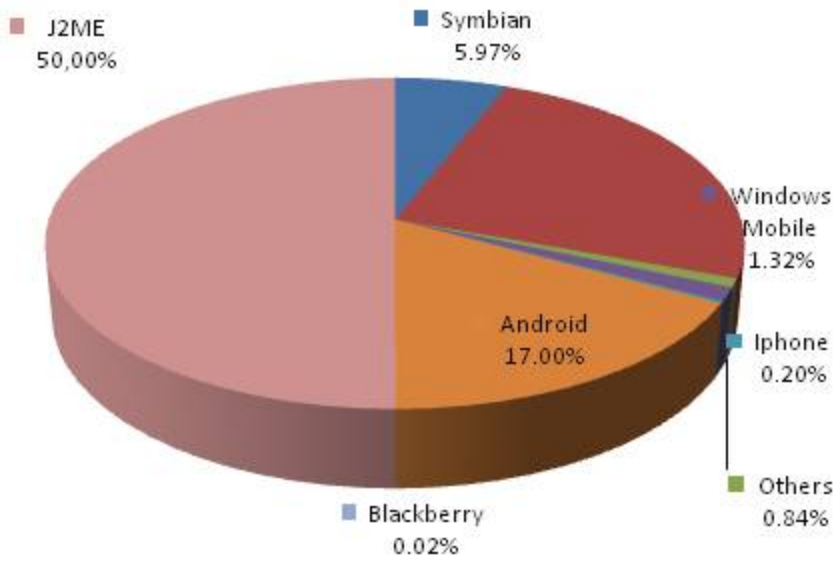
Source: Kaspersky Lab September 2011

Mobile malware

Some statistics

- Number of mobile malware families to date: **314**
- Number of mobile malware modifications to date: **3052**
- Mobile malware found in August 2011: **314 new modifications (new record!)**
- Most common mobile threat: **SMS trojans**

Mobile malware written for specific platforms:



Source: Kaspersky Lab 26th September 2011

5 Social Media Mania

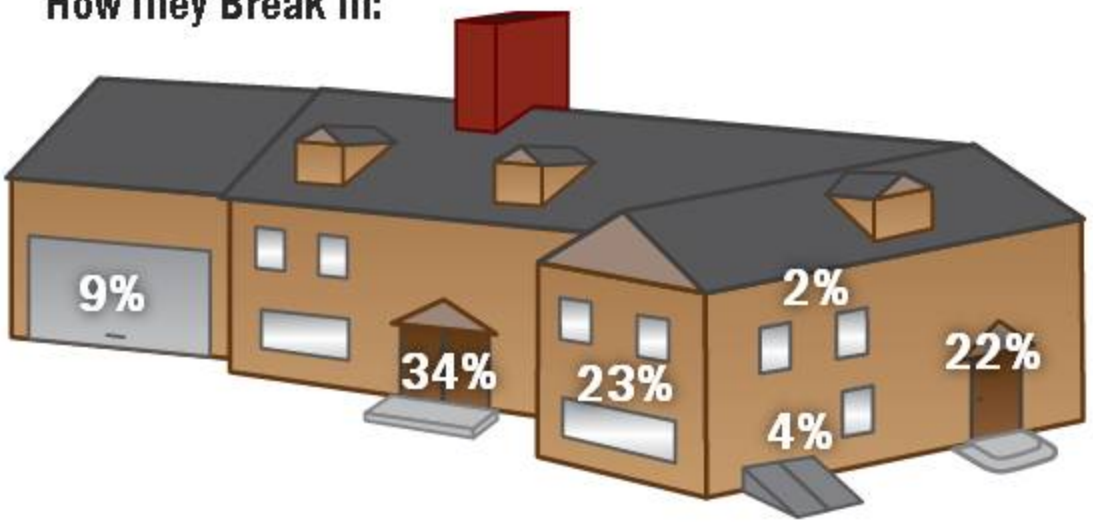
Adopting Social Media Without Protection

6 Attention Misdirection

Focusing on Prevention vs. Detection and Response

- 95% of respondents listed the 12 items below
- 95% thought that Prevention was key
- IT Security spending follows the same mindset

How They Break In:



Prevention		Detection		Response	
Doors	Locks	Alarm	Motion detector	Dog	Gun
Windows	Fence	Monitoring	Crime watch	Police	Insurance

Source: "Data @ Risk" by David H. Stelzl

7 Awareness Deficit

Failing to foster a culture of awareness

8 Threat Camouflage

Underreporting of security breaches

"According to the FBI, cybercrime officially cost Americans almost $560 million last year, more than double the 2008 tally, although experts say the true number is undoubtedly much higher, since **many cyberattacks go unreported.**"

– Dallas Morning News, May 2, 2010

9 Compliance Complacency

Settling for Compliance

> Compliance... just one step north of **negligence**.
>
> *– Josh Corman, The 451 Group*

COBIT

PCI Security Standards Council

Sarbanes-Oxley

HIPAA.ORG

NIST

Children's Internet Protection Act

10 Assuming Everything is OK

How many times have you heard your IT team say:

"We're covered...
We are compliant"

only to have your expensive external audit firm come in and deliver a scathing report that enumerates thousands of missed items, erroneous configurations, and process violations?

10 Fallacies about Endpoint Security

1	Data Center Fixation	Assuming the data is in the data center
2	Information Amnesia	Forgetting the value of data on mobile devices
3	Migration Myopia	Believing that company data never finds its way to home systems
4	Device Dyslexia	Treating mobile devices as desktops
5	Social Media Mania	Adopting of social media without protection
6	Attention Misdirection	Focusing on Protection versus Detection and Response
7	Awareness Deficit	Failing to foster a culture of awareness
8	Threat Camouflage	Under-reporting of security breaches
9	Compliance Complacency	Settling for compliance
10	Assuming Everything is OK	Always get a second opinion!

Kaspersky Endpoint Security

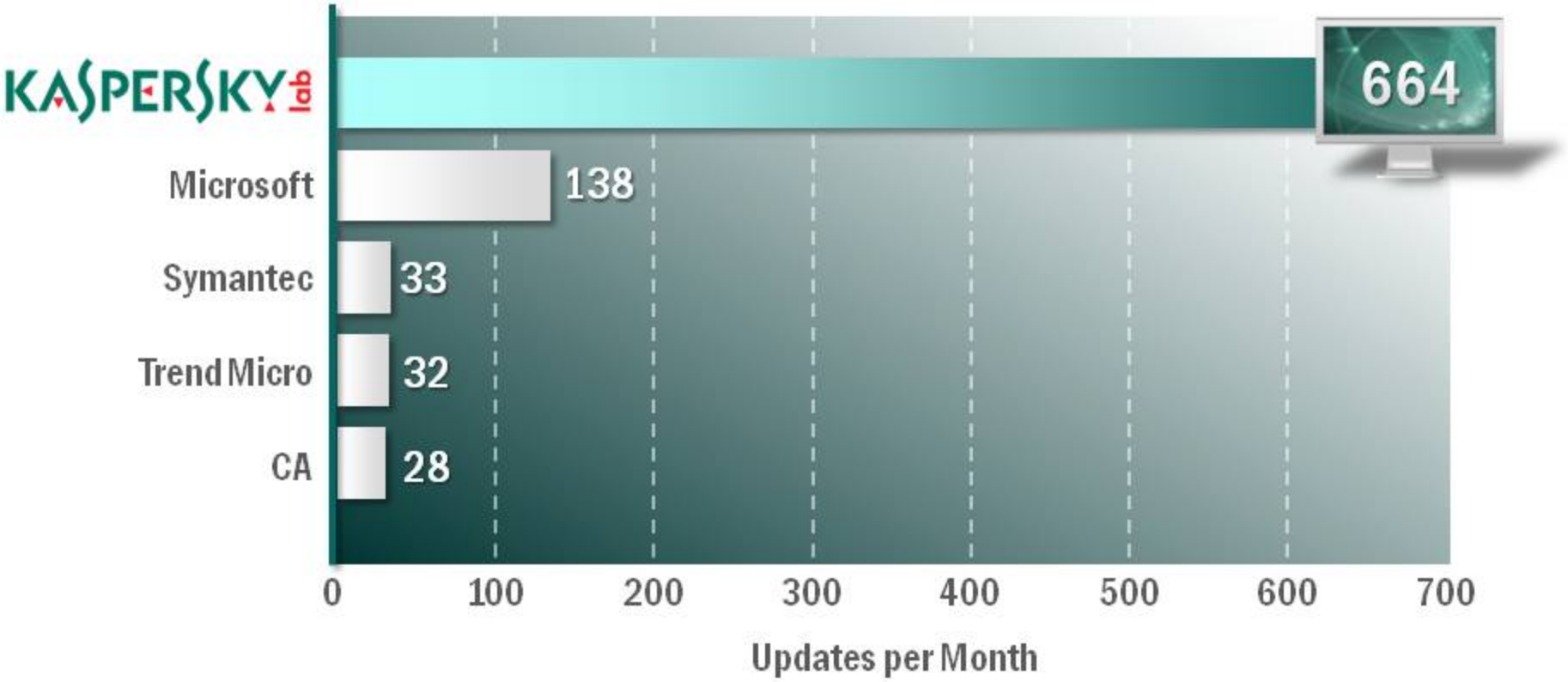
Visibility

Control

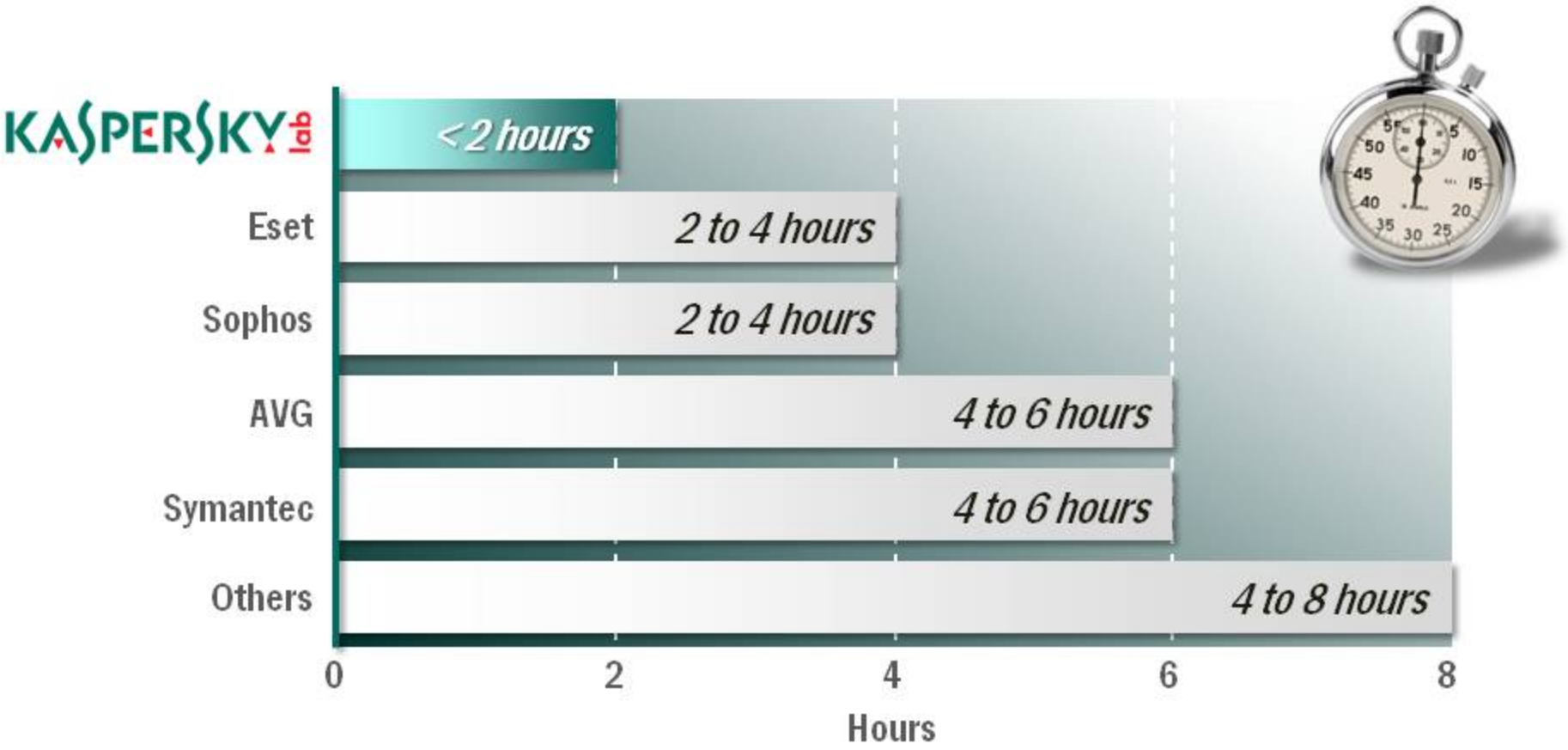
Protection

The Most Immediate Protection

Small Updates for the Best Protection and User Experience



Fastest Response Time to New Threats



Source: AV-Test.org

Layered End-to-End Protection