Business IT Security

Threats, technologies & solutions

Adrian Porcescu, Technical Consultant EM & Trainer, Kaspersky Lab
InfoCom Security, April 10, 2013

TODAY'S AGENDA

KASPERSKY lab

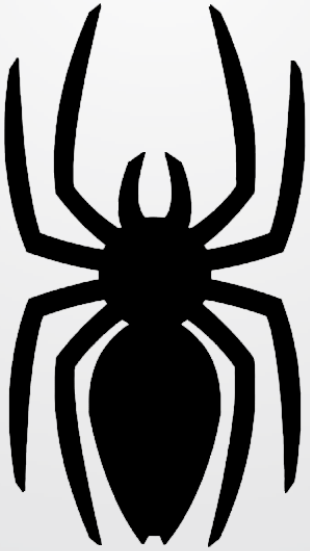
Malware evolution

Let’s take a look at it!

MALWARE IS HUGE

1994

One new virus every hour

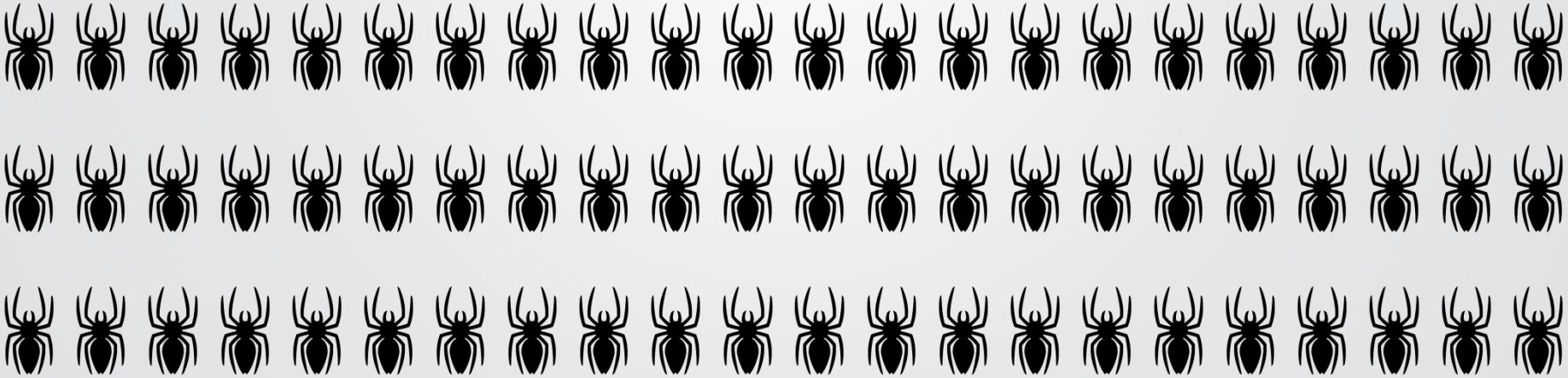


KASPERSKY lab

MALWARE IS HUGE

2006

One new virus every minute



KASPERSKY lab

MALWARE IS HUGE

2012

One new virus every second

Or 100.000 samples/day

What about

2013

?

Kaspersky Lab

is currently processing

200.000

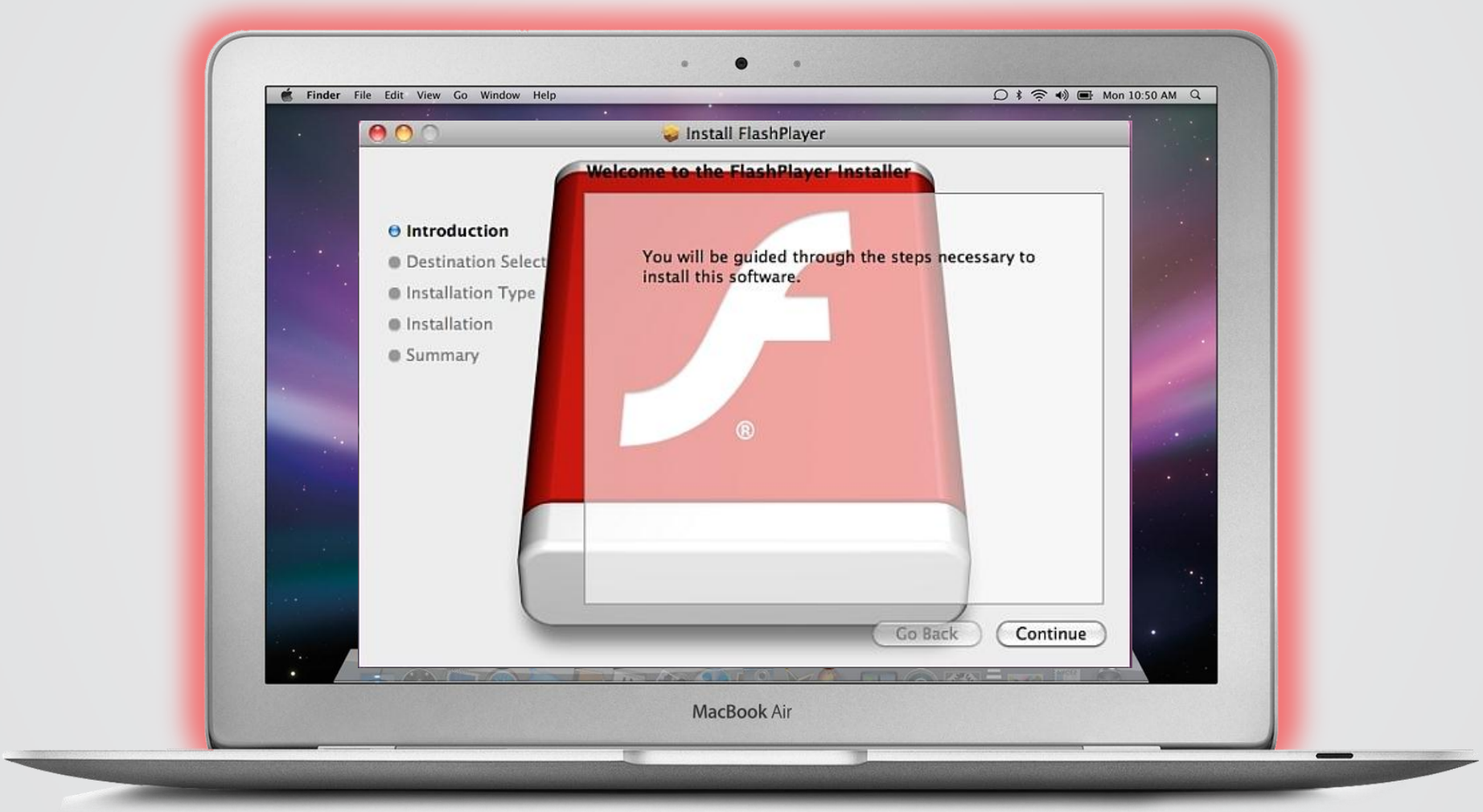
unique malware samples

EVERY DAY

Traditional cybercriminals

are now targeting emerging platforms

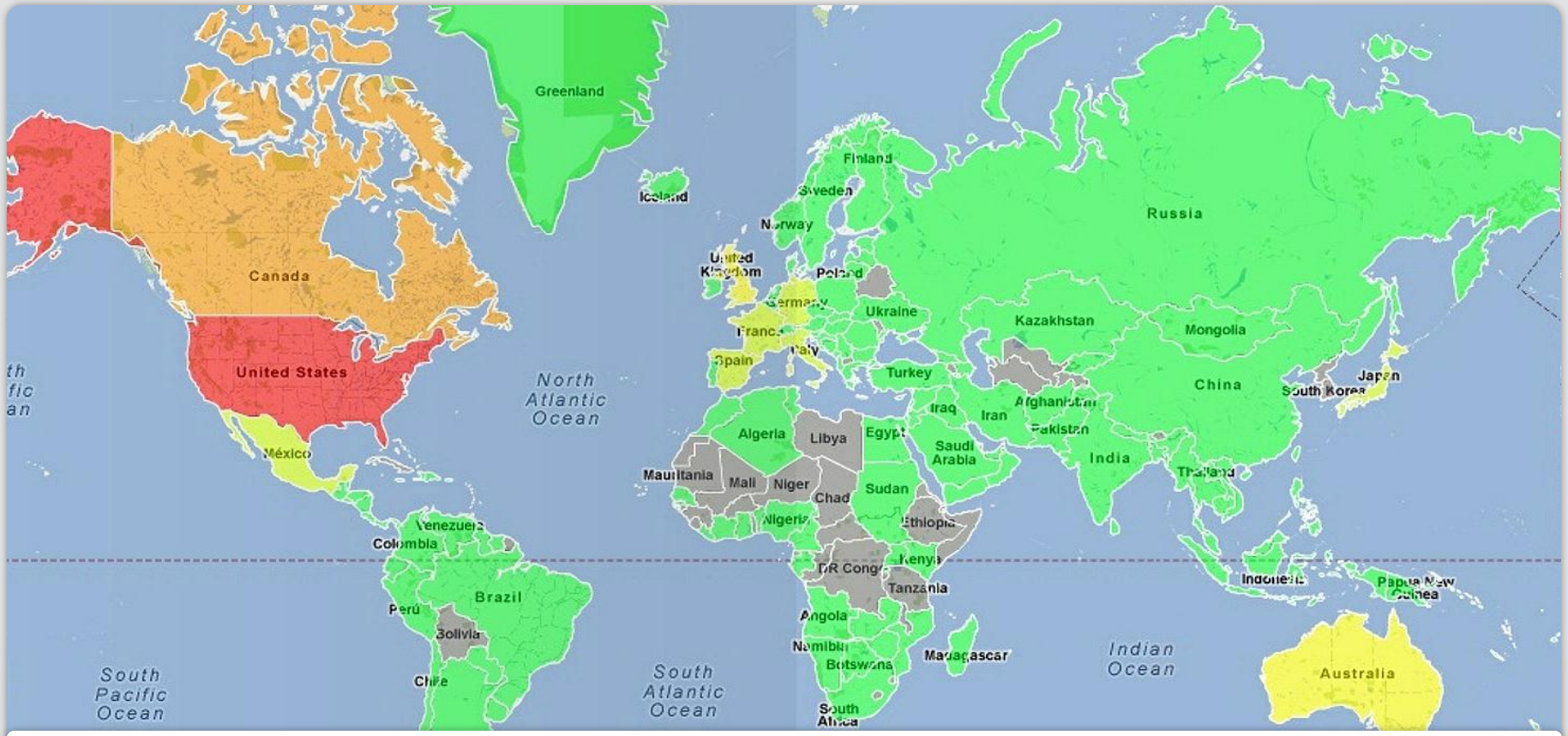
WHEN FLASHFAKE STARTED…



KASPERSKY lab

TROJAN-DOWNLOADER.OSX.FLASHFAKE

How did FlashFake manage to infect +700.000 Macs?



94,625 – 300,917	47,109 – 94,625	7,891 – 47,1097	2,547 – 7,891	1 – 2547

KASPERSKY lab

Mobile malware

has become a reality.

WHAT ABOUT MOBILE MALWARE?

2004 – 2010

1160 mobile malware samples

2011

6193 mobile malware samples

December

2137 mobile malware samples

2011 was a year of mobile malware

What about 2012?

KASPERSKY lab

WHAT ABOUT MOBILE MALWARE?

2004 – 2010

1160 mobile malware samples

2011

6193 mo
malware s

Dece

2137 r
malw
sampl

In 2012 we've discovered +30000 malicious files for mobiles

What about 2012?

KASPERSKY

Cyber warfare

Espionage and sabotage have now moved online

What are we protecting?

The trend: Nation state sponsored attacks are on the rise.

2009 **Aurora**

2010 **Stuxnet**

2011 **Duqu**

2012
- Flame
- Gauss
- miniFlame
- Shamoon

CONCLUSIONS AND PREDICTIONS

Malware will continue to grow exponentially YoY

As long as there's a way to make money out of it, cybercriminals will always create malware

Malware now moving towards emerging platforms

Google's Android and Apple's OS X have never been more targeted by cybercriminals

Cyber-espionage and cyber-sabotage, a common thing

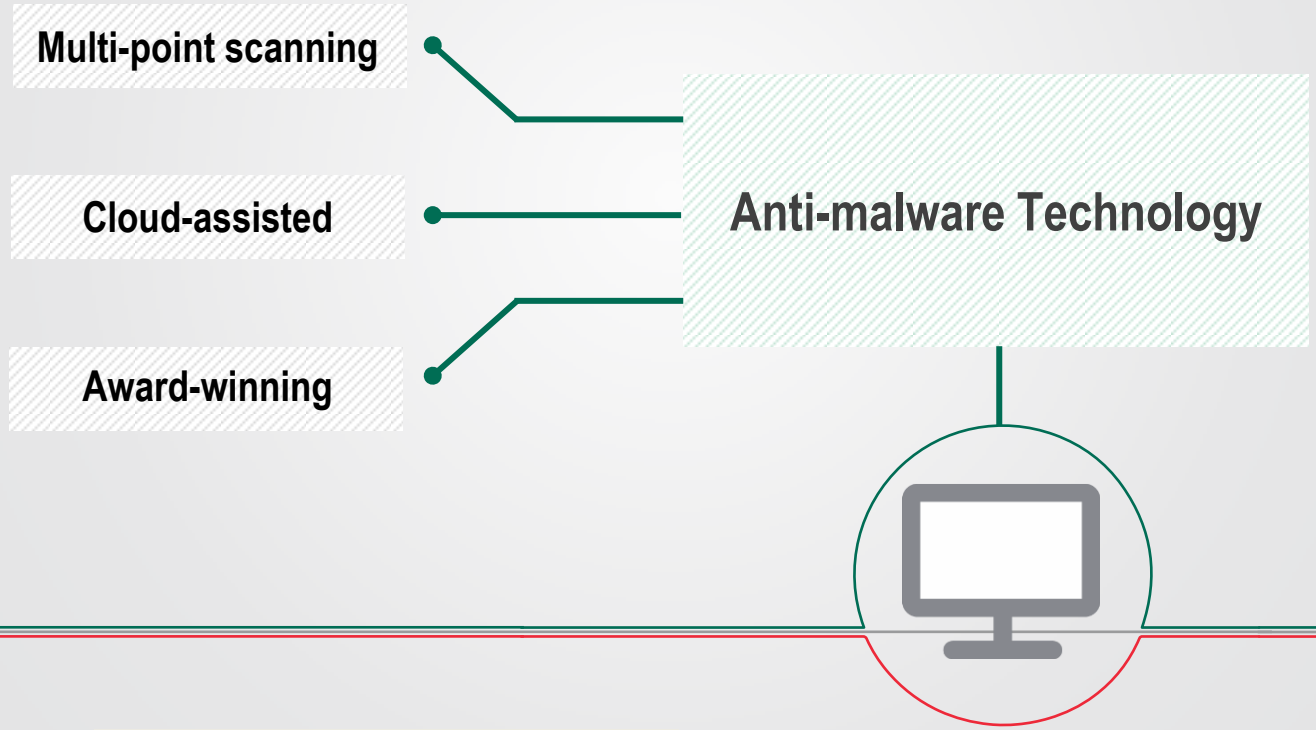
Nation states are currently building defensive (and offensive) cyber capabilities

Technologies

Protection, control & management

Anti-malware

- The foundation of the platform



Automatic Exploit Prevention test efficiency by MRG Effitas

	Exploit 1	Exploit 2	Exploit 3	Exploit 4	Exploit 5	Exploit 6	Exploit 7	Exploit 8	Exploit 9	Exploit 10	Exploit 11	Exploit 12	Exploit 13
Kaspersky Endpoint Security for Business	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kaspersky Internet Security 2013 AEP Only	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Symantec Norton Internet Security 2012	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
AVG Internet Security 2012	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Eset Smart Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Trend Micro Titanium Maximum Security 2012	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
Avira Internet Security 2012	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
McAfee Total Protection 2012	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
Microsoft Security Essentials V4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
F-Secure Internet Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗
Bitdefender Internet Security	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗

KASPERSKY lab

Application Control with Default Deny

A new approach to enhanced IT security

Application Control is...

An advanced security technology for businesses that helps:

- Minimize the cost of maintaining network security
- Enhance the efficiency of corporate resource usage
- Improve protection against targeted attacks
- Manage software by categories, according to your security policy

Default Deny — game-changing protection

- Blocks all programs except those that have been specifically allowed
- Dynamic whitelisting technology provides greater control over software
- Makes execution of unauthorized code virtually impossible

KASPERSKY lab www.whitelist.kaspersky.com

Evaluating Application Control

Independent industry specialists West Coast Labs invited 7 vendors to take part in the industry's first deep testing:

Accepted the invitation

- Kaspersky Lab
- Symantec
- McAfee
- Fourth vendor*

Declined the invitation

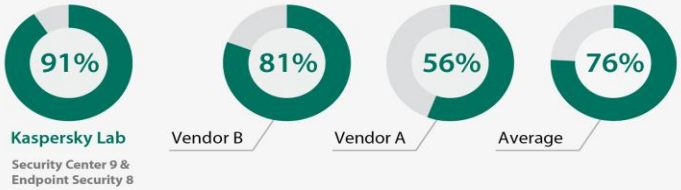
- Lumension
- Bit9
- Coretrace

A weighting system was introduced for easier **evaluation** of results.

* A vendor who participated in the testing but then, subsequent to the testing being completed, requested to withdraw

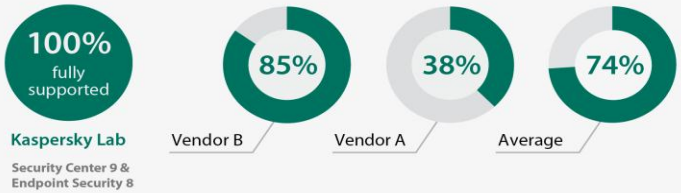
Application Control test results

Kaspersky Lab, McAfee, Symantec *



* indicates how fully the technology was implemented by a certain vendor

Default Deny test result



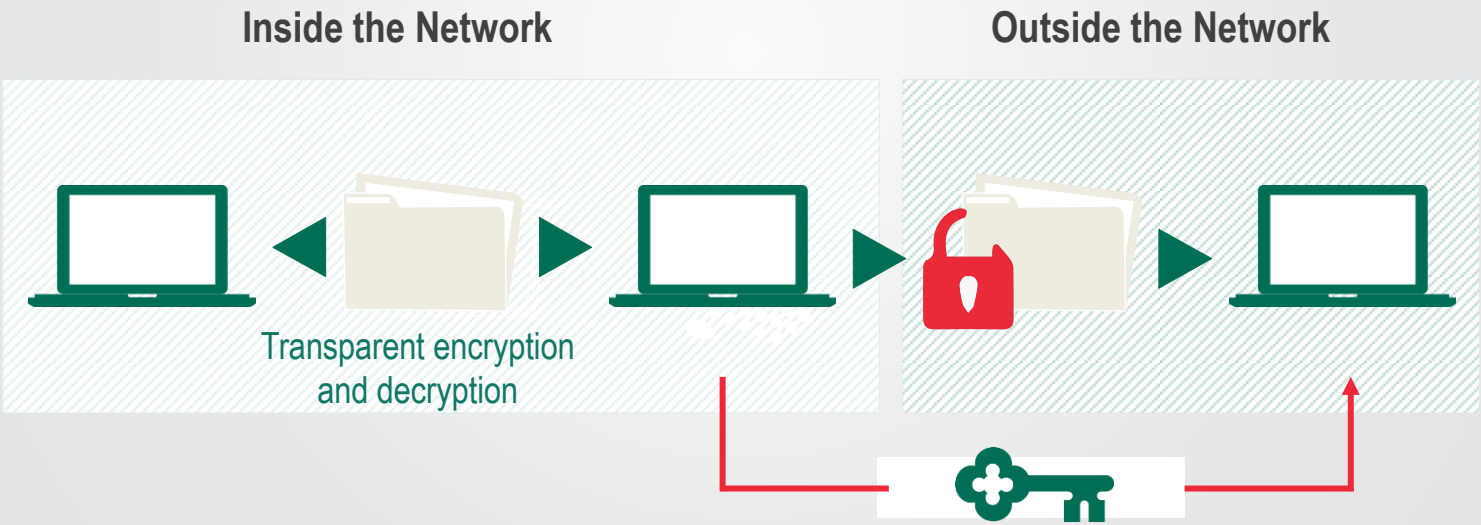
KASPERSKY lab

Data encryption

Keeping your data safe, wherever it goes

Encryption features

- File / folder or full-disk
- Transparent to end-users
- Integrates with device control and application control



Mobile security

Anti-Malware

Anti-Theft

Policy Enforcement

Data Protection

Systems management

- Staying up-to-date just got faster and easier

SYSTEM PROVISIONING

- Create images
- Store and update
- Deploy

LICENCE MANAGEMENT

- Track usage
- Manage renewals
- Manage licence compliance

REMOTE TOOLS

- Install applications
- Update applications
- Troubleshoot

VULNERABILITY SCANNING

- HW and SW inventory
- Multiple vulnerability databases

ADVANCED PATCHING

- Automated prioritisation
- Reboot options

NETWORK ADMISSION CONTROL (NAC)

- Guest policy management
- Guest portal

Solutions

Main factors

Technological factor

Human factor

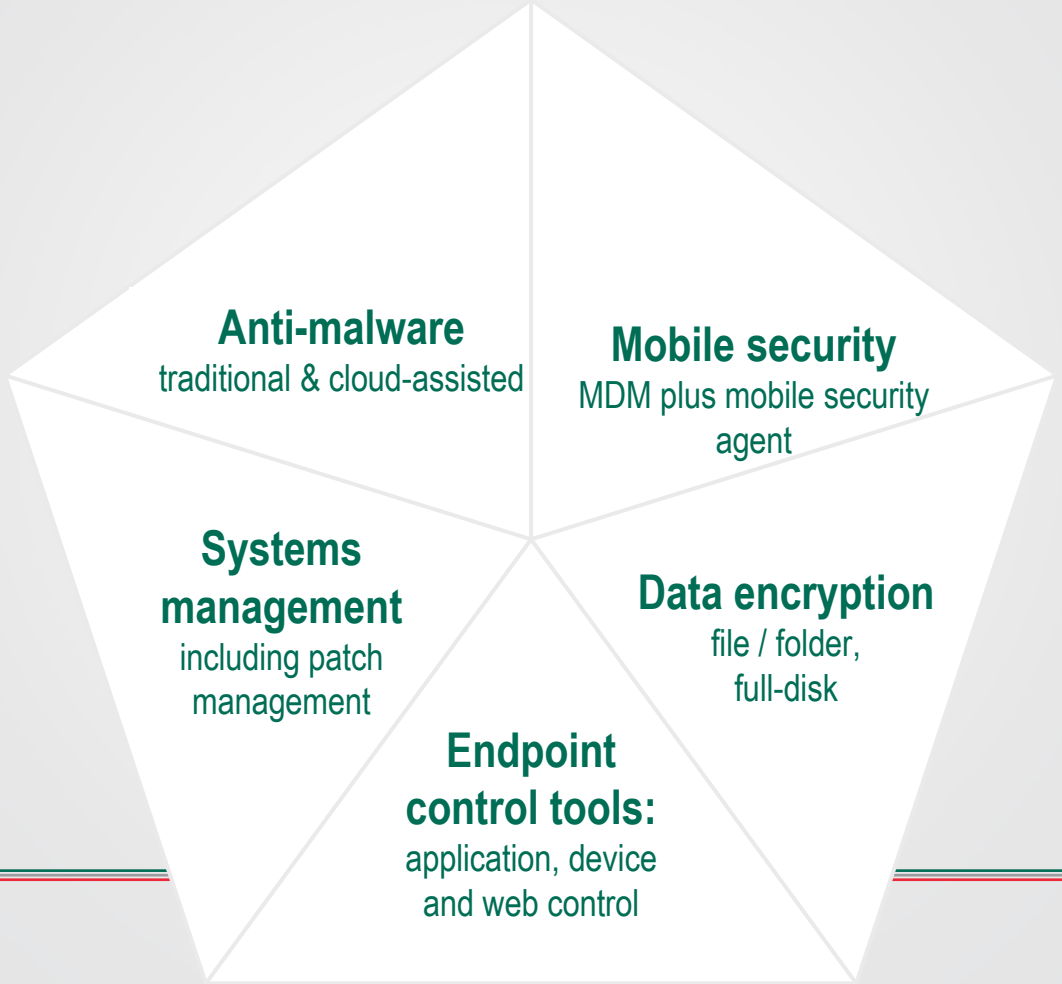
KASPERSKY lab

Technological factor

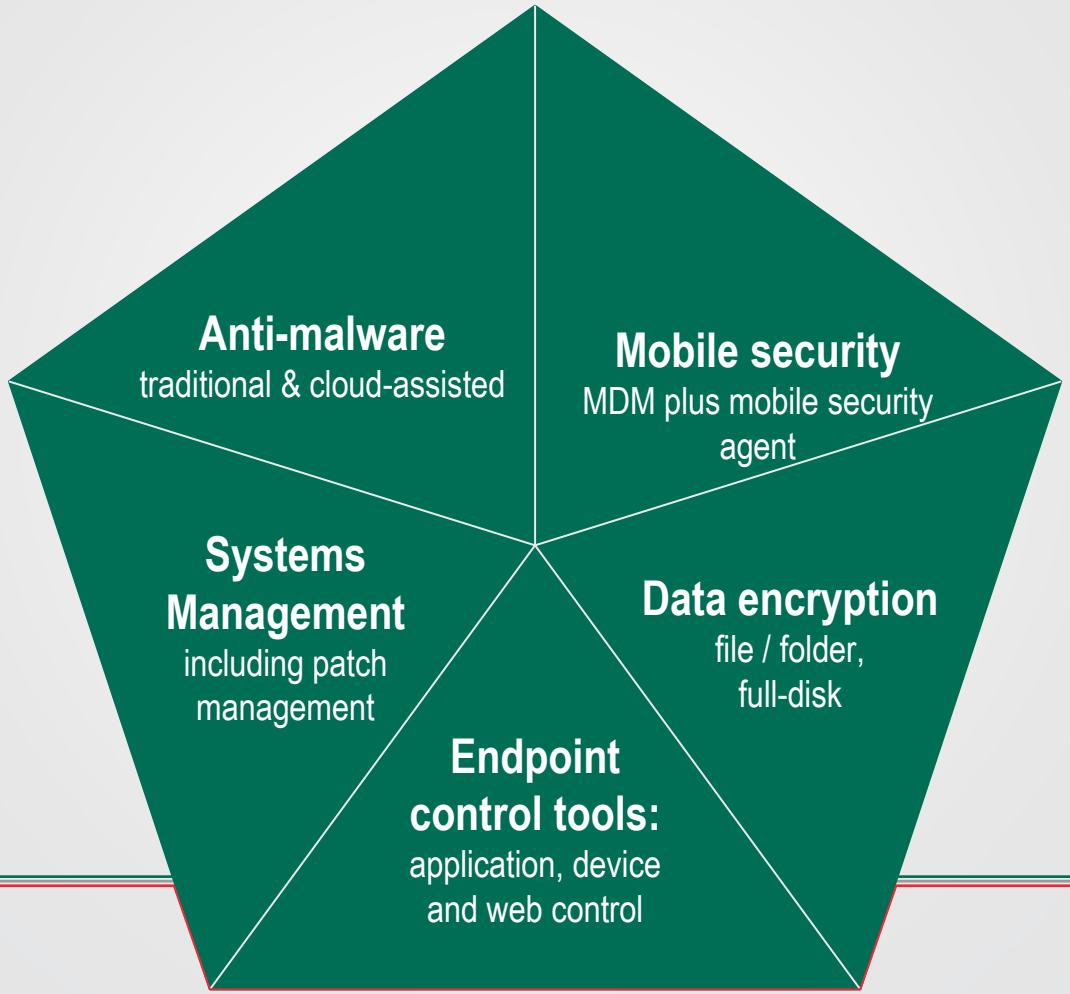
Chose the technological partner, not the marketing one

KASPERSKY lab

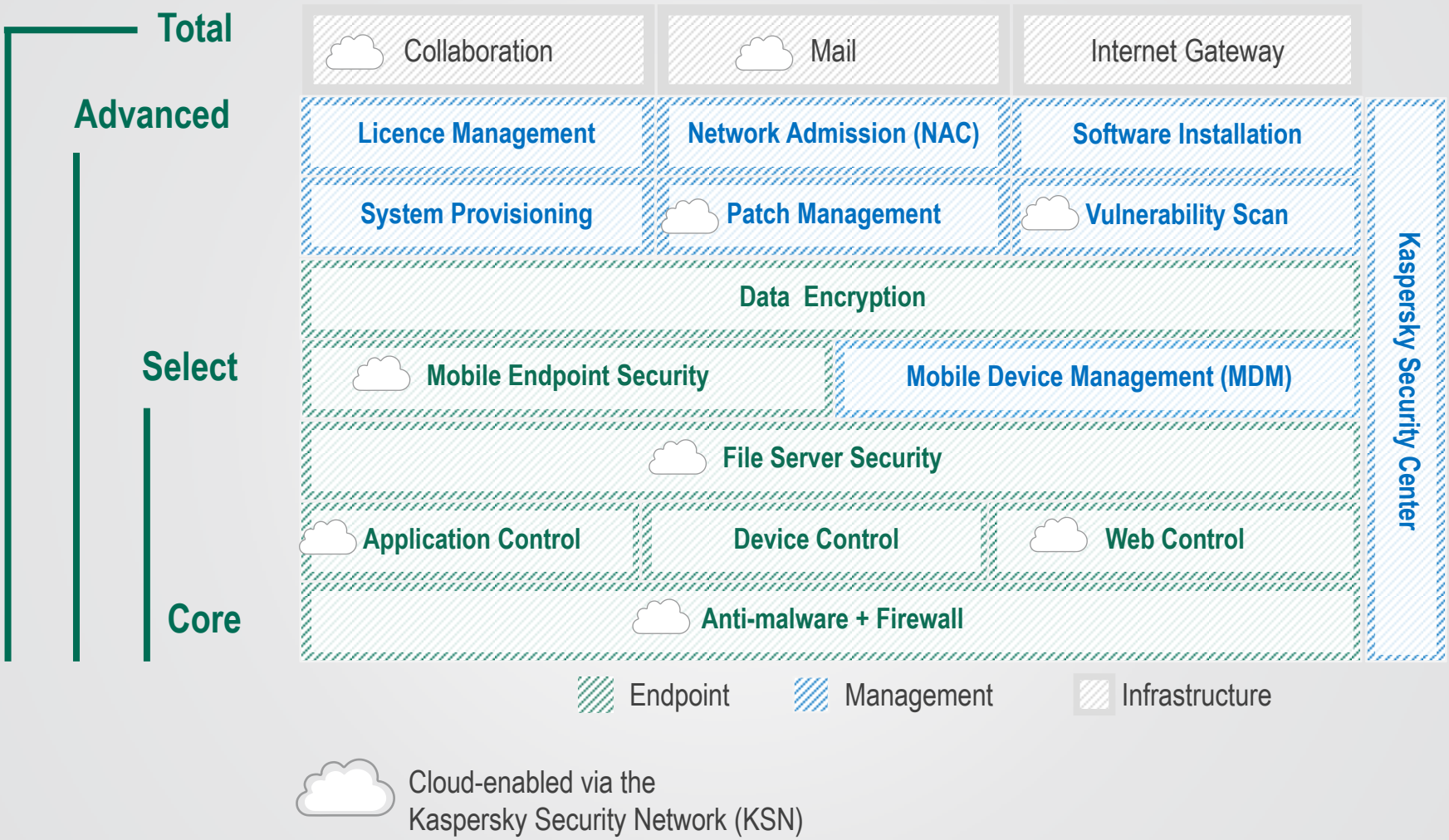
One single platform that contains:



All managed through a single management console



Kaspersky Endpoint Security for Business:



Human factor

Education

- www.securelist.com/blog
- www.secureviewmag.com
- www.threatpost.com
- support.kaspersky.com

KASPERSKY lab

Thank you!

Questions?

Adrian Porcescu, Technical Consultant EM & Trainer, Kaspersky Lab
InfoCom Security, April 10, 2013

KASPERSKY lab