

It Takes a Village

Reducing the Threat Gap by Allying with Your Competition

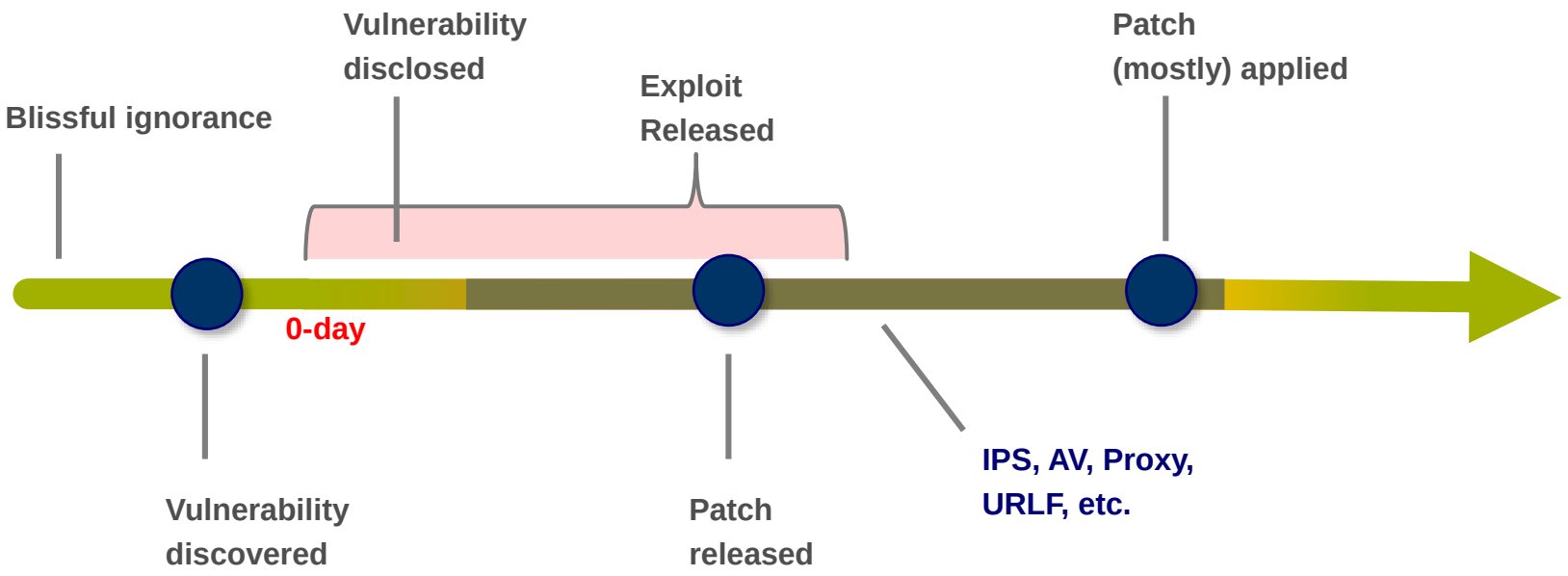
Presented by: Scott Maring (smaring@checkpoint.com)

Developed by: Michael A. Barkett (mbarkett@checkpoint.com)

SecTor: October, 2013

©2013 Check Point Software Technologies Ltd.

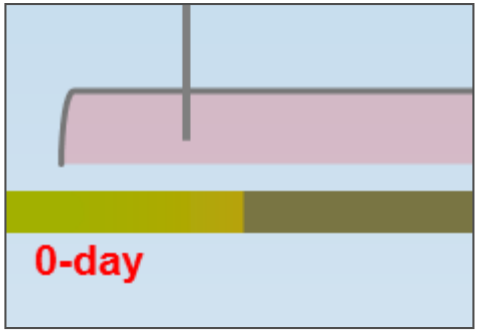
Foundation: The Patch Gap

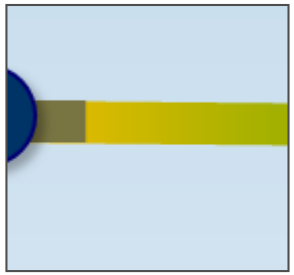


- 0-day is relevant from the moment an exploit exists
  - Regardless of whether the vendor is aware
- Patching is a window, not a point in time

©2013 Check Point Software Technologies Ltd.

It Never Ends: The Threat Gap





- Attackers more determined, sophisticated
- More precise targeting
- 0-day became a real threat

©2013 Check Point Software Technologies Ltd.

We fight back, but staying ahead is difficult…

- Can’t proxy the entire Internet, so we add technology



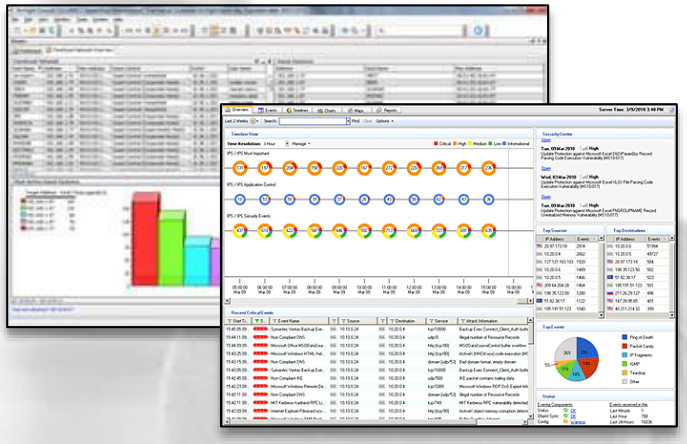
IPS



App FW



Anti-bot





Web Security



DLP



URLF



Anti-spam

The Unpredictable Nature of Users



- Too many logs?
- How are you correlating the massive amount of information?
- Trusted vs. untrusted (BYOD complications)

©2013 Check Point Software Technologies Ltd.

Let’s breathe some life into the situation!



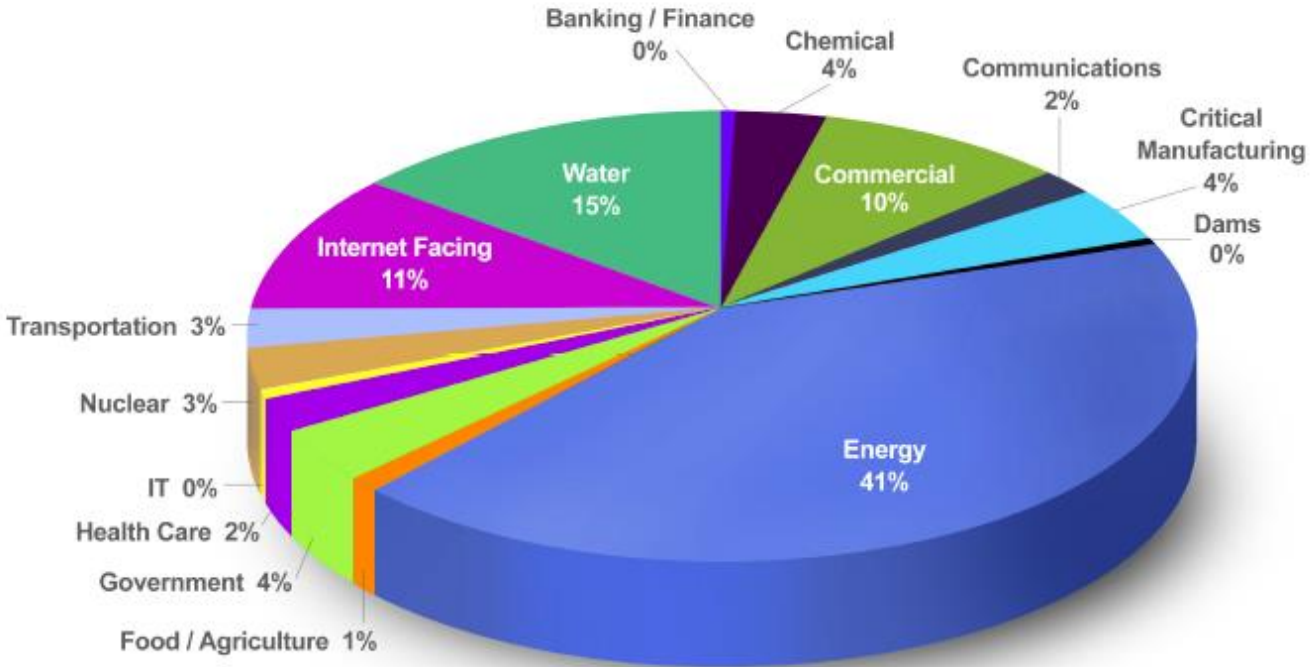
©2013 Check Point Software Technologies Ltd.


COLLABORATION
TOGETHER
SUCCESS
HELP
WORK
PEOPLE
GOAL
SOURCES
POLITICAL
SOFTWARE
PROJECT
SECTION
COMMUNICATION
COMMUNITIES
SOCIAL
PEER
GROUPS
UNITED
INCLUDE
INDUSTRY
BETWEEN
INTERNET
TERM
BENEFITS
PRODUCTION
ORGANIZATION
CORPORATION
KNOWLEDGE
COLLABORATIVE
TOOLS
ORGANIZATIONS
BASED
LEARNING
MANAGEMENT
CITATIONS
PRACTICE
COMPLEX
PROJECTS
DEVELOPMENT
THEORY
PERFORMANCE
WORKING
COMMUNITY
MEMBERS
INDIVIDUAL
RESOURCES
SHARED
SHARING
IMPROVE
ADDING
INCLUDING
CHALLENGED
RELIABLE
SCIENTIFIC
TRADE
SKILLS
IDEAS

Industry Applicability

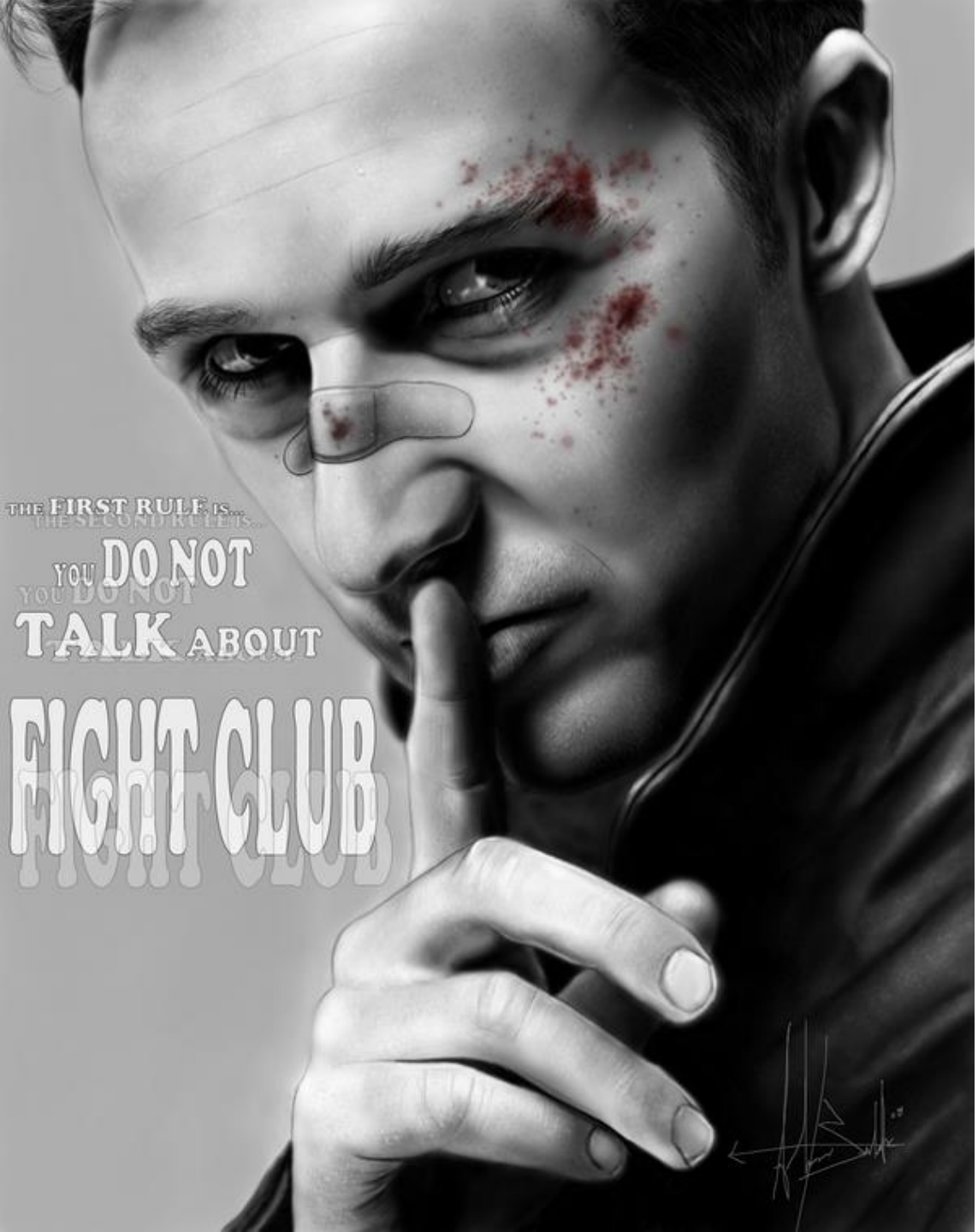
Check Point SOFTWARE TECHNOLOGIES LTD.

Healthcare & Financial Services?



2012: SCADA / Critical Infrastructure

©2013 Check Point Software Technologies Ltd.



Check Point
SOFTWARE TECHNOLOGIES LTD.

How can we collaborate?

- ISACs
- Don’t discuss the details of the proceedings
- Actively participate!
- Be truthful and forthcoming
- No product pitches
- Shirts and shoes ok

©2013 Check Point Software Technologies Ltd.

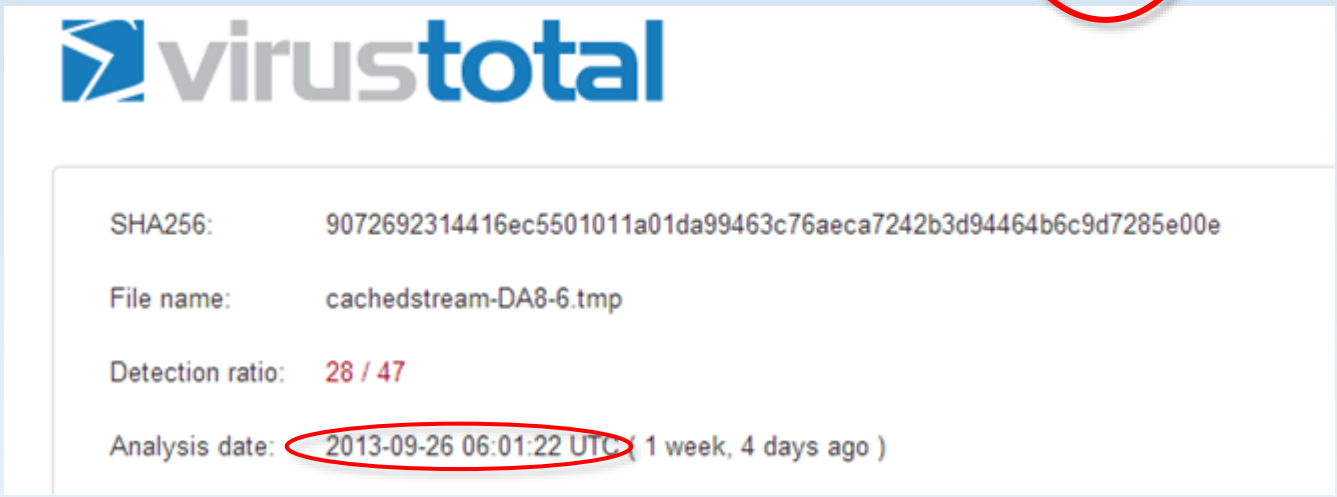
The World's Largest Neighbourhood Watch



Ephemeral: Flash in the pan

- Customized for a specific moment in time
- Designed to evade detection

Country	Attack Name	Number of reports	First seen	Last seen
PT	c960035c42e5e6097bd828dad777aad6	27	2013-07-29 10:31:15.0	2013-07-29 14:14:41.0
IL	c960035c42e5e6097bd828dad777aad6	22	2013-07-29 11:23:58.0	2013-07-29 13:40:31.0
US	c960035c42e5e6097bd828dad777aad6	7	2013-07-29 12:08:19.0	2013-07-29 13:08:19.0



©2013 Check Point Software Technologies Ltd.

Real-time Collaboration Regardless of Industry Vertical

Check Point SOFTWARE TECHNOLOGIES LTD.

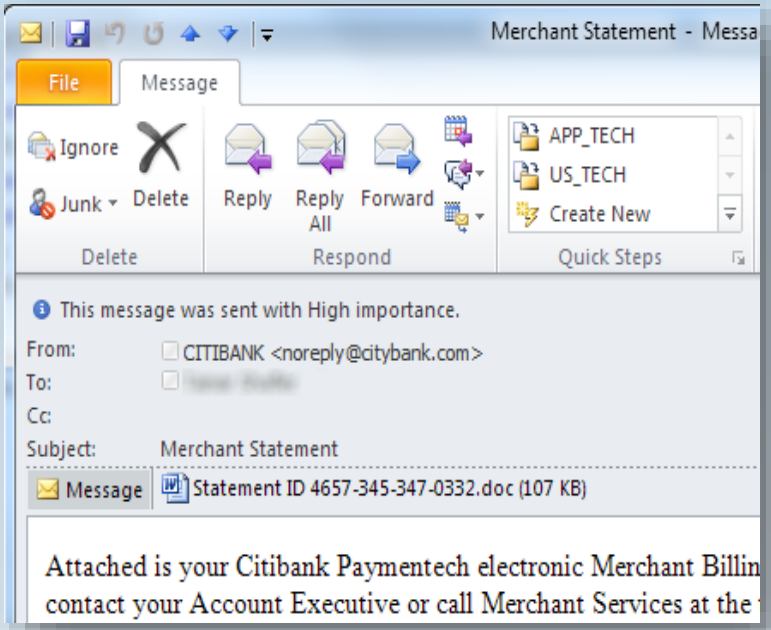


Real-time sharing for immediate protection

©2013 Check Point Software Technologies Ltd.

Real-world Zero-Day: Findings

- Over 50 unique instances in the same day
- Nearly 1000 **targeted** attack attempts originated from domains such as:
  - Collegeclub.com
  - Injersey.com
  - Teacher.com
  - Techauto.net
  - Wiredsolutions.net



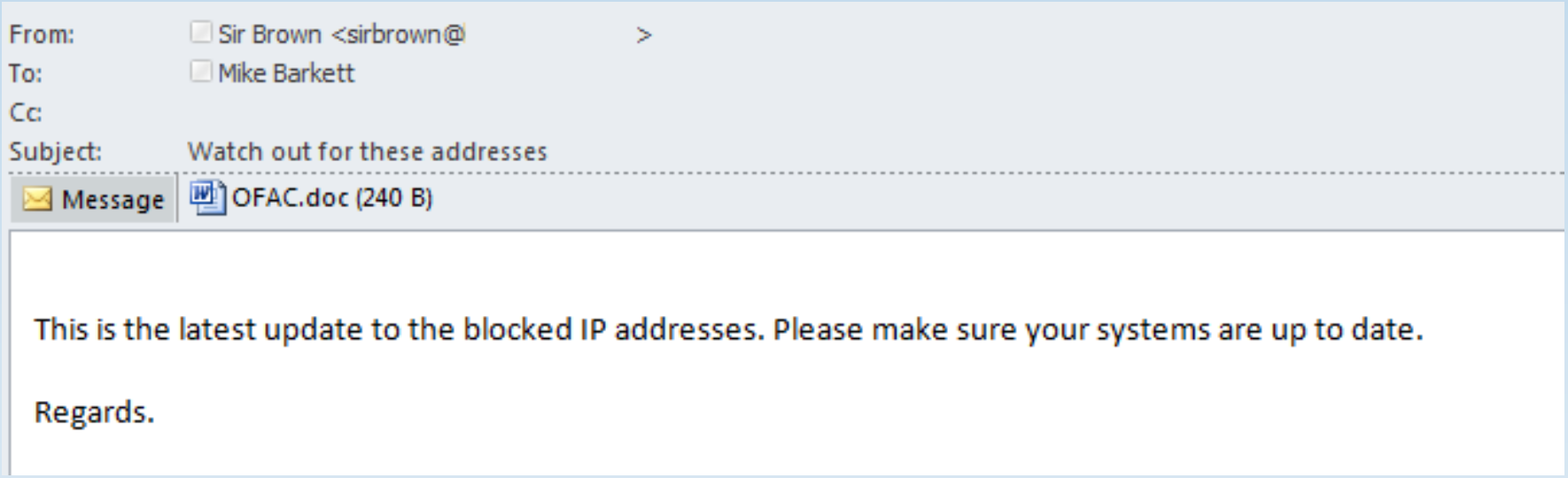
- Threat Emulation detected characteristics such as files and processes created or destroyed, etc.

- More info: http://www.checkpoint.com/threatcloud-central/security-talk/te-discovery.html

©2013 Check Point Software Technologies Ltd.

Real-world Example

- Never before seen document, late July, 2013:



- Turns out it is malware
- Creates processes, replicates, steals passwords, etc.

©2013 Check Point Software Technologies Ltd.

The Alliance

Global **Sharing** of Symptoms



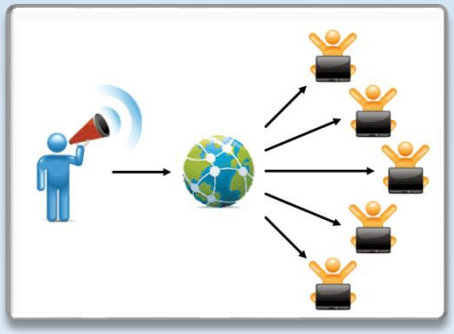
Malware Research



Signature Development



Update all gateways



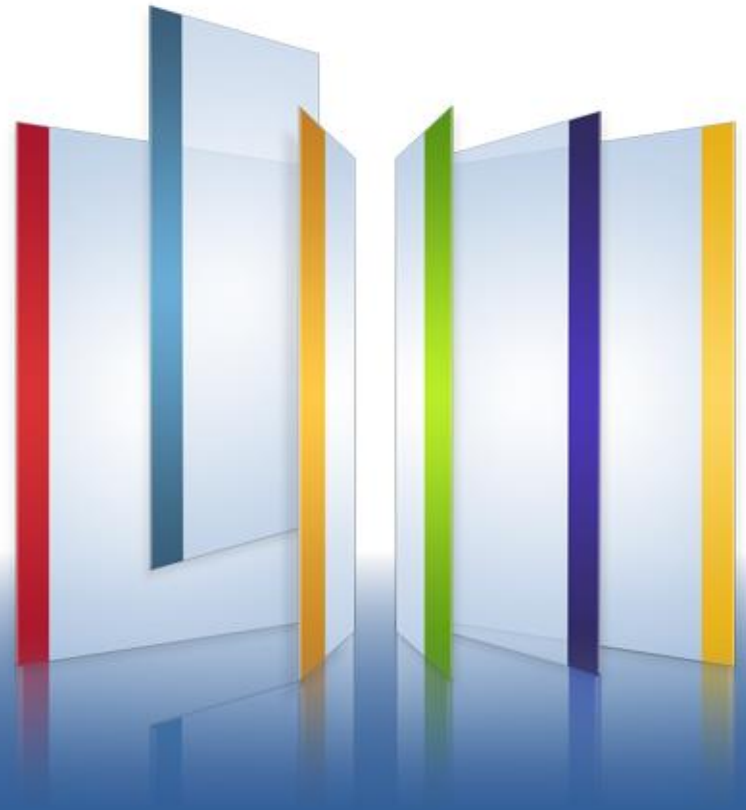
- >100k enterprise customers
- Millions of hosts

Collaboration of Data ← → Research ← → Distribution

©2013 Check Point Software Technologies Ltd.

Q&A

Image credits
Oak tree: http://fc01.deviantart.net/fs28/f/2008/133/7/c/Oak_tree_by_attila0427.jpg
Collaboration: http://www.emergenetics.com/wp-content/uploads/2013/08/Strucutural-Collaboration.jpg
Fight Club Fan Art: http://www.fanpop.com/clubs/fight-club/images/8474492/title/first-rule-fanart



Thank you!

Scott Maring (smaring@checkpoint.com)

SecTor: October, 2013

©2013 Check Point Software Technologies Ltd.