TREND MICRO™

Securing Your Web World



Security in the Clouds

Latest Trends of Internet Security Threats and its Implications to Taiwan

Steve Chang

Cyber Attack – Latest Weapon of Mass Destruction

On July 4, 2009, US and South Korea government networks were besieged for days by a coordinated attack from hundreds of thousands machines.

Web Sites Affected

White House
US State Department
US Dept. of Homeland Security
US Secret Services
US Dept. of Treasury
New York Stock Exchange
Washington Post
S. Korea Office of President
S. Korea National Assembly
Korea Exchange Bank

How it Started? – Social Engineering Attacks

時間：96年7月18日 (星期三) 上午9:30－12:00

地點：國家高速網路中心南部事業群 3F虛擬實境廳

住址：台南縣新市鄉南科三路28號

報名專線:http://ww.twisc.ncku.edu.tw線上報名(至7月16日截止)

為解決傳統網路安全測試平台之不足，結合美國Utah大學所授權提供的軟體、國產硬體以及自行研發設計的軟體與韌體，提供國內資訊安全研究與實驗所需的隔離性、封閉性、可紀錄性、可控制性與可儲存性之完整環境。本次會議將介紹Testbed@TWISC 發展成果，並透過實際的操作演示來展現Testbed@TWISC對資安研究的支援能力，期能為國內學術資安研究提供良好的測試、研發與教學環境。

會 議 議 程：

96年7月18日 (三)			
時間	**行程**	**主講人**	**地點**
9:30-9:50	報到		國網
9:50~10:00	貴賓致詞	李德財院士 陳如芬主任	3F虛擬實境廳
10:00~10:20	Testbed@ TWISC介紹	賴溪松教授	3F虛擬實境廳
10:20~11:00	Testbed@ TWISC Demo	賴溪松教授	3F虛擬實境廳
11:00~11:15	Testbed@TWISC設備參觀	國網6F機房	國網6F機房
11:20~12:00	Testbed@TWISC未來；座談與討論	李德財院士、陳如芬主任、賴溪松教授	3F虛擬實境廳

Identifying an Associated Contact

國立成功大學 教師資料 Faculty Data
National Cheng Kung University

賴溪松 教授

職稱

教授

電話

+886-6-275-7575 ext. 62369

傳真

+886-6-234-5482

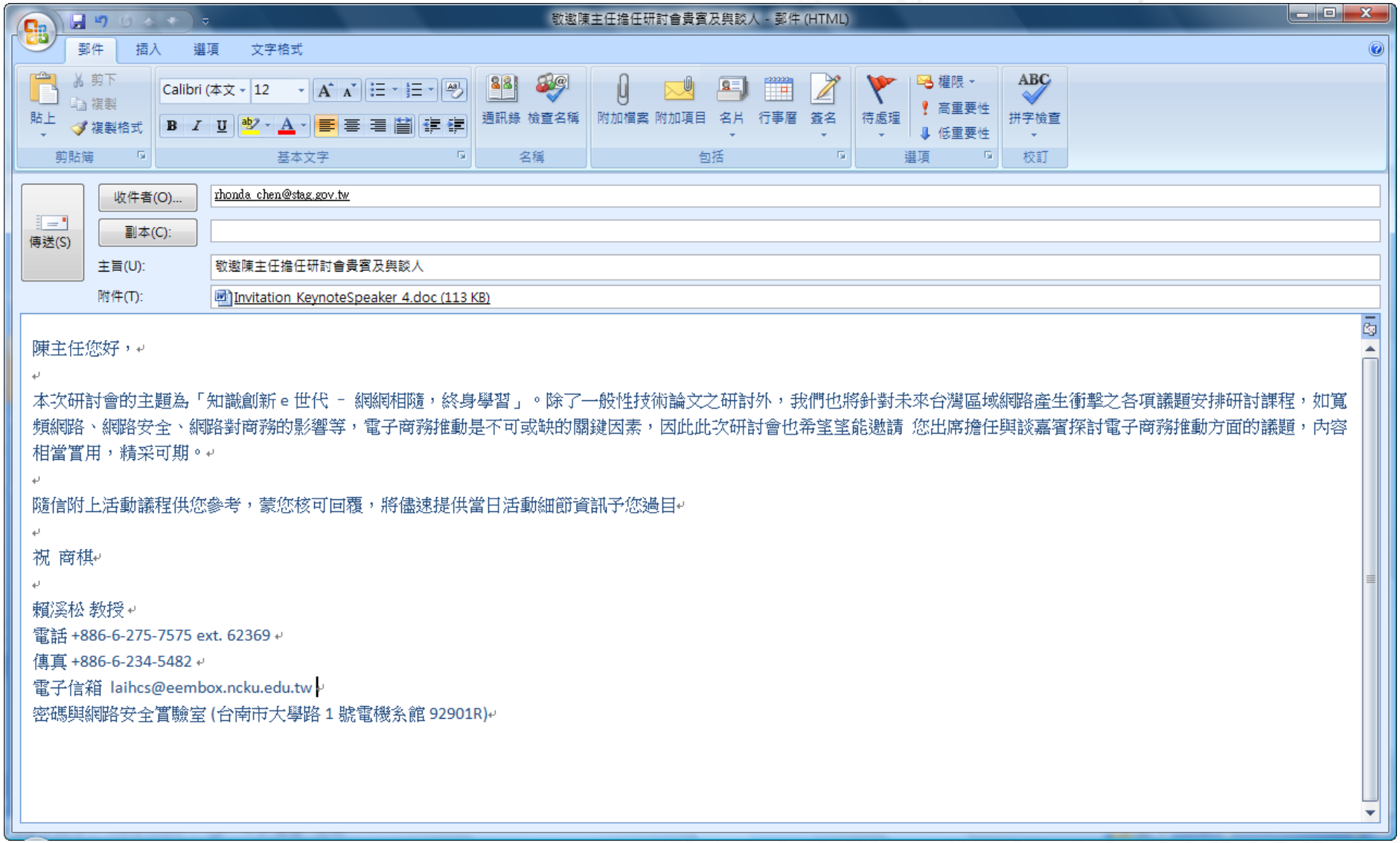
電子信箱

laihcs@eembox.ncku.edu.tw

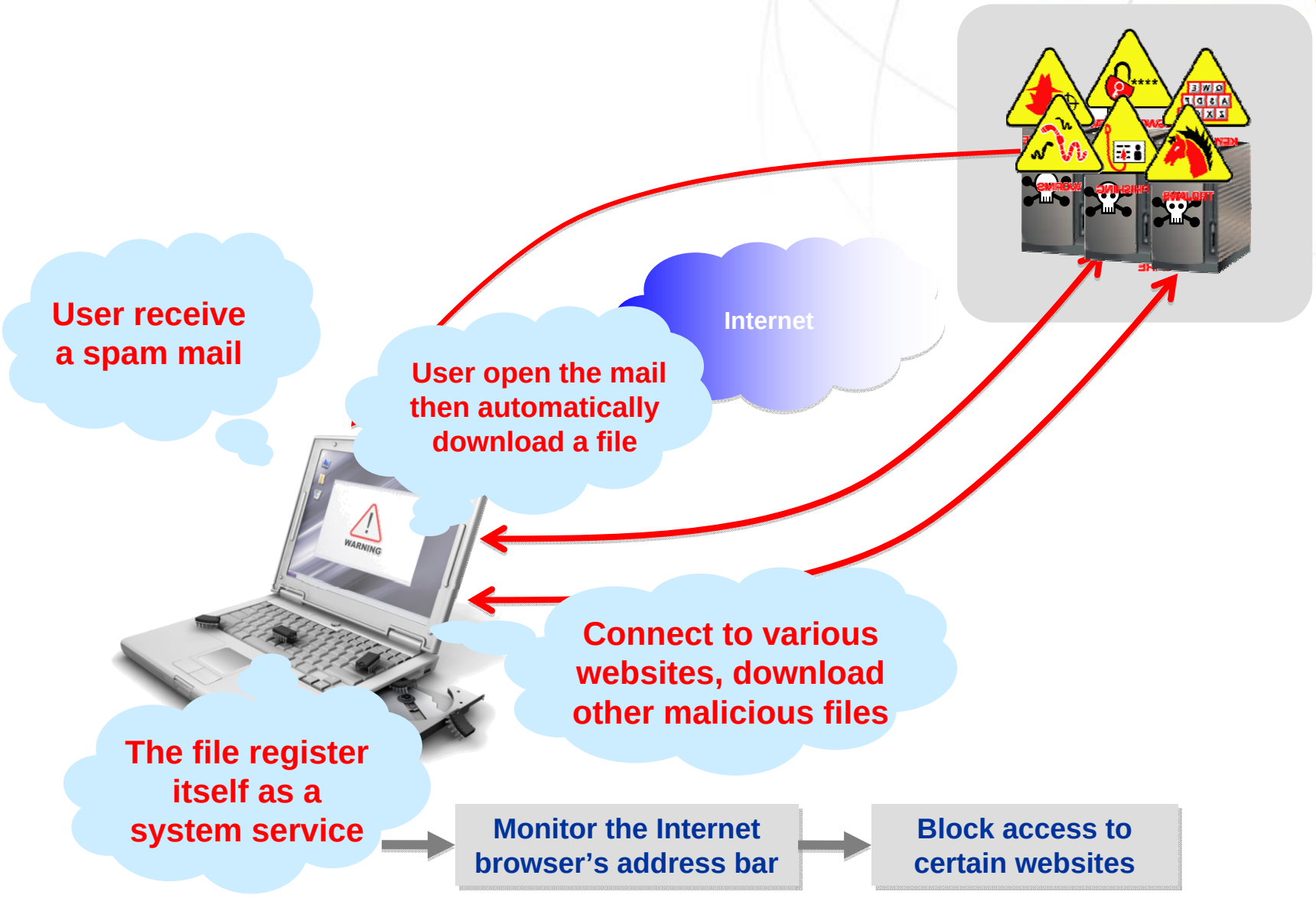
實驗室

密碼與網路安全實驗室 (台南市大學路1號電機系館92901R)

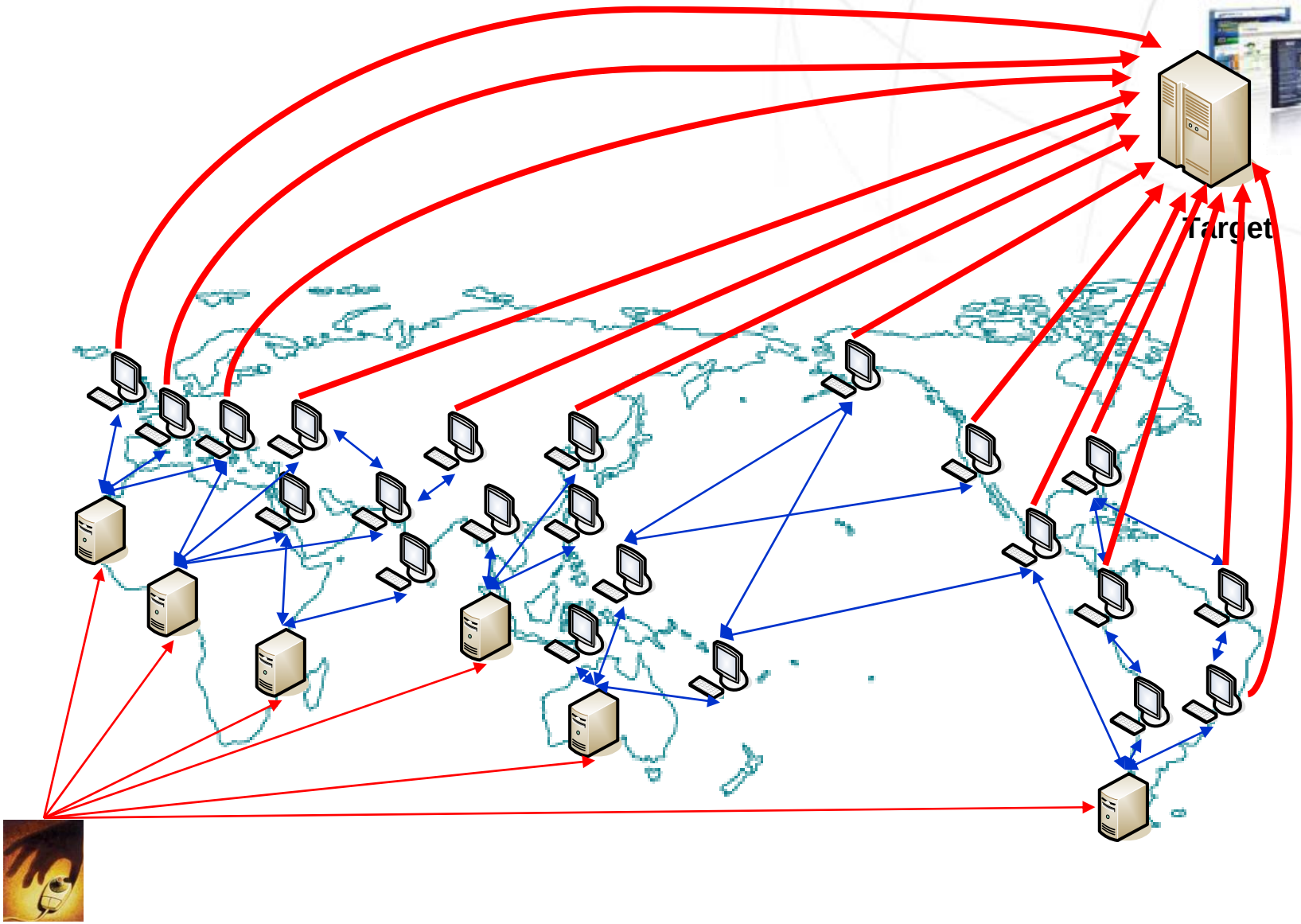
Then Send a Fake Email with a Trojan Horse



Launching the Conficker / Downadup Attack

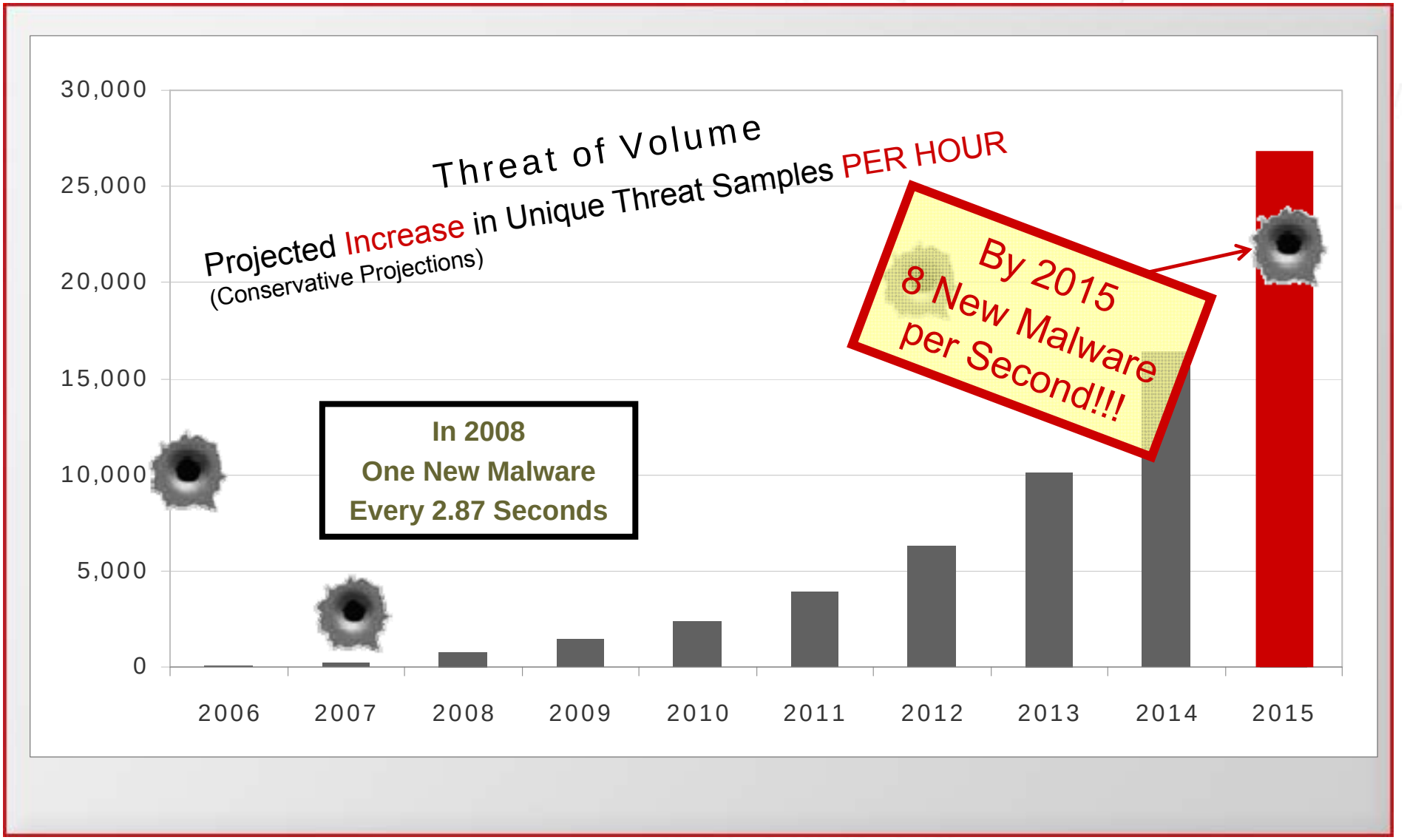


Attack from the Cloud – DDoS Attack

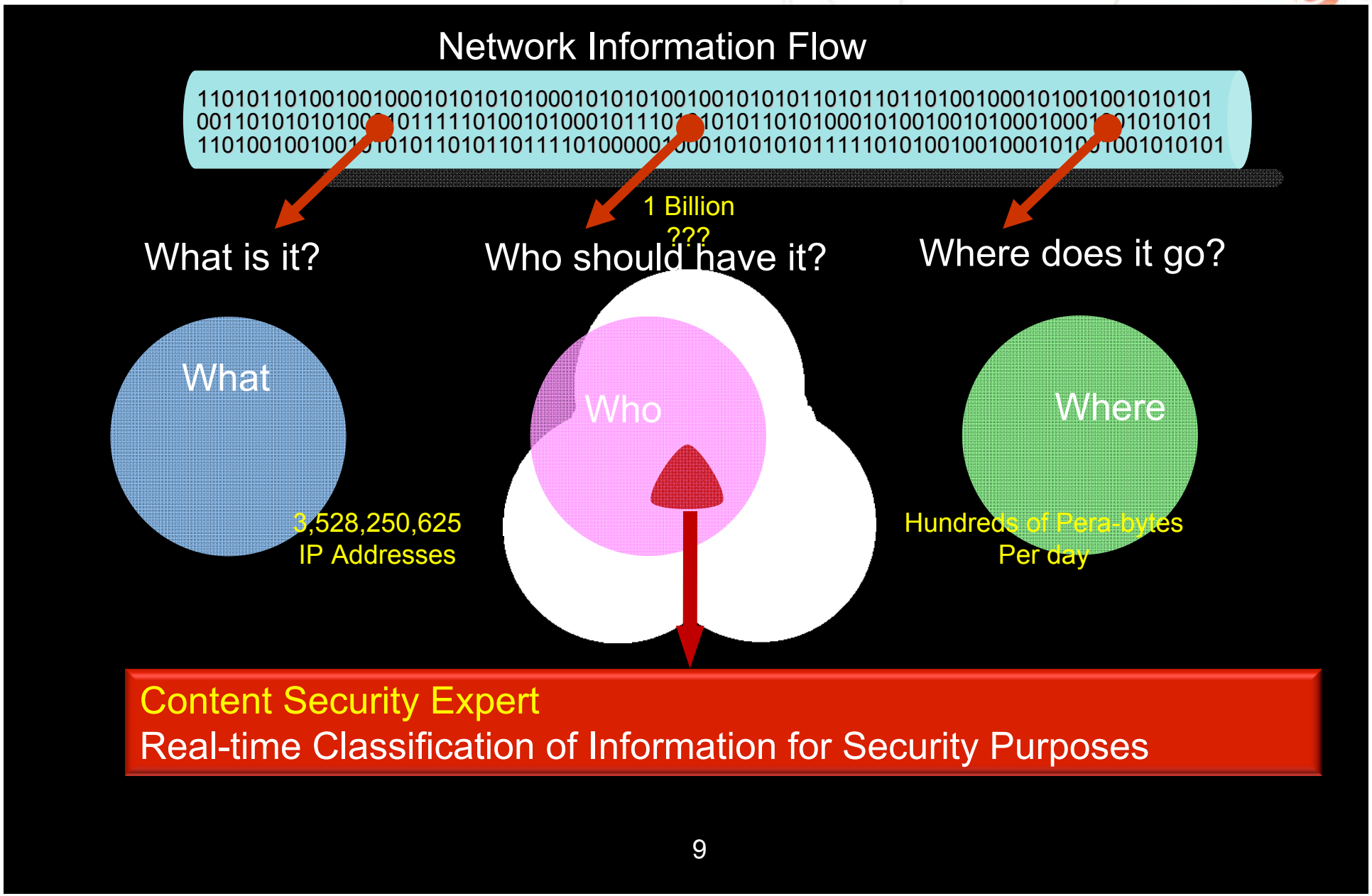


Cyber Terrorist

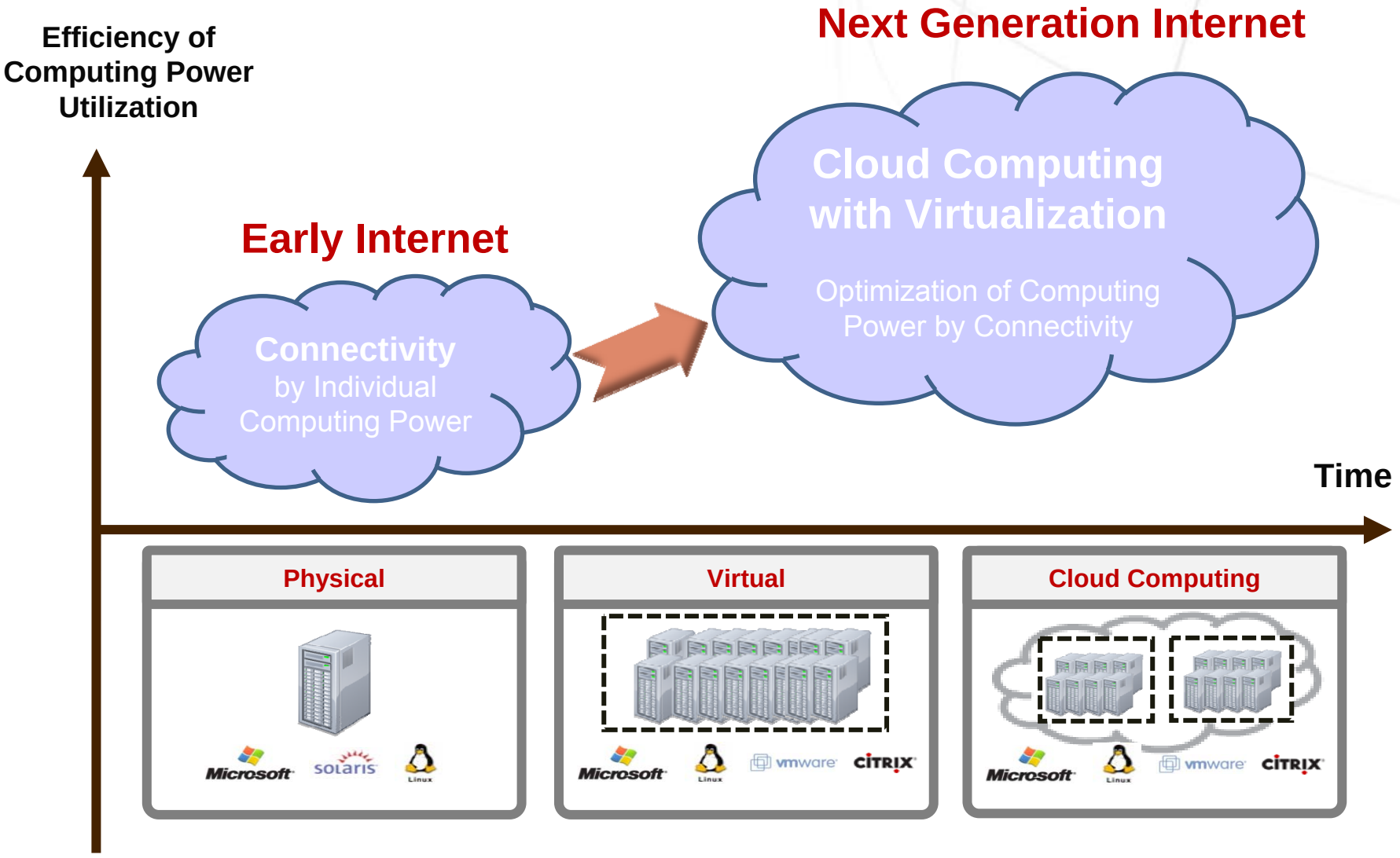
Number of Malware is Multiplying



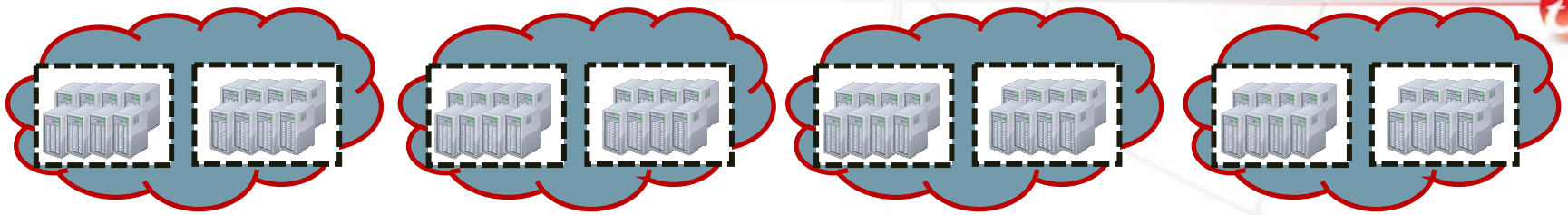
Defending the Cloud



Using Cloud to fend off Attacks from the Cloud



Protection From the Cloud

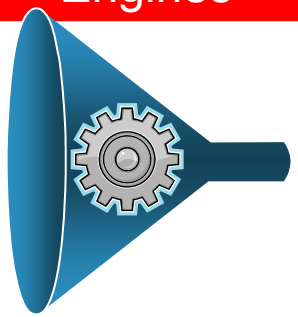


Threats Intelligence

Global Threat Detection Network

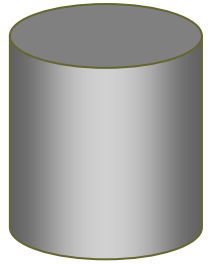
- Millions of Sensors
- Globally Distributed
- Unique Coverage
- Multi-Threat

TrendLabs Correlation Engines



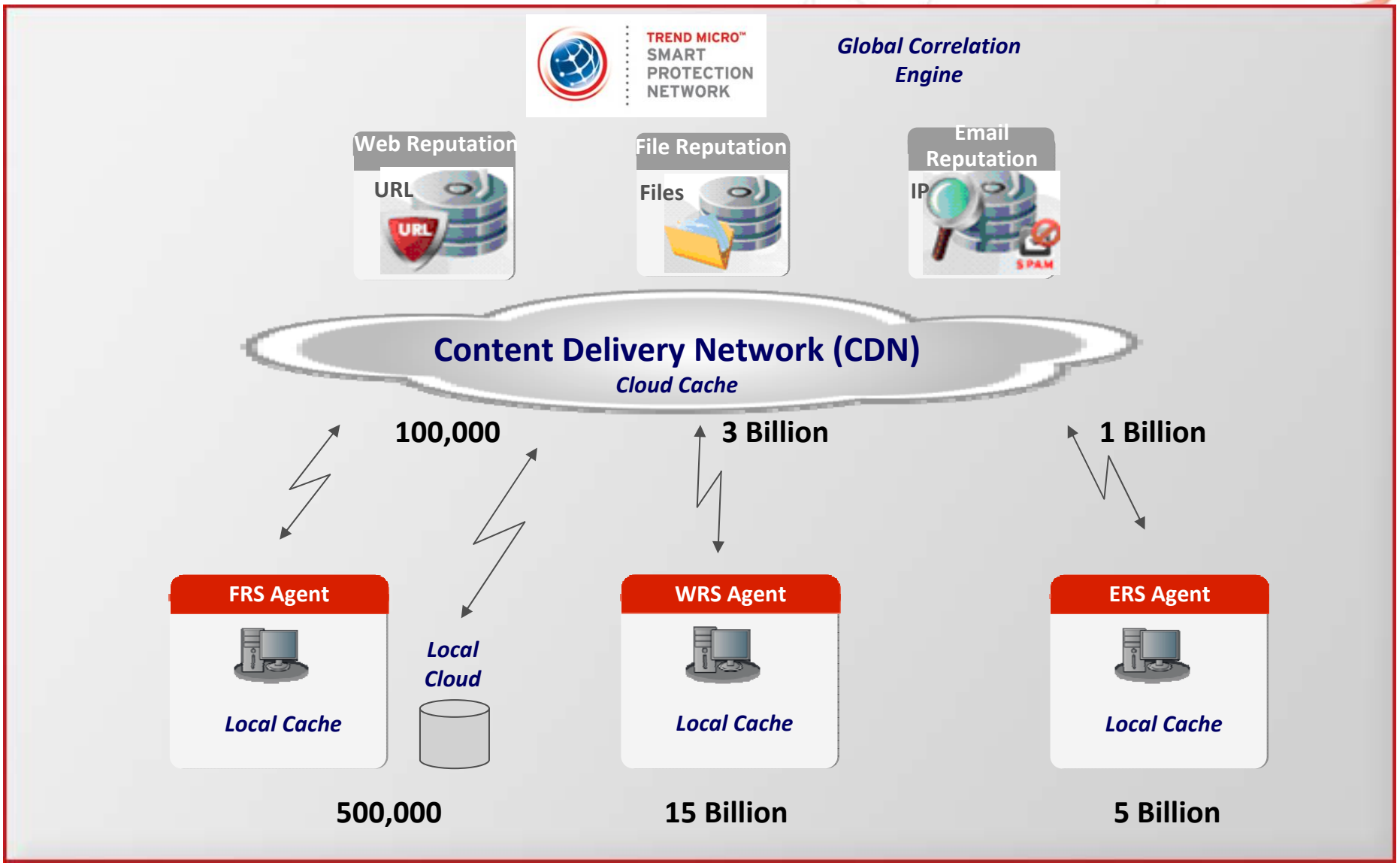
- 100% Trend Micro Technology
- Correlates results from:
  - Anti-Spam
  - Anti-Malware
  - Webcrawl
  - Honeypots
- Global Data centre Network

Dynamic Database

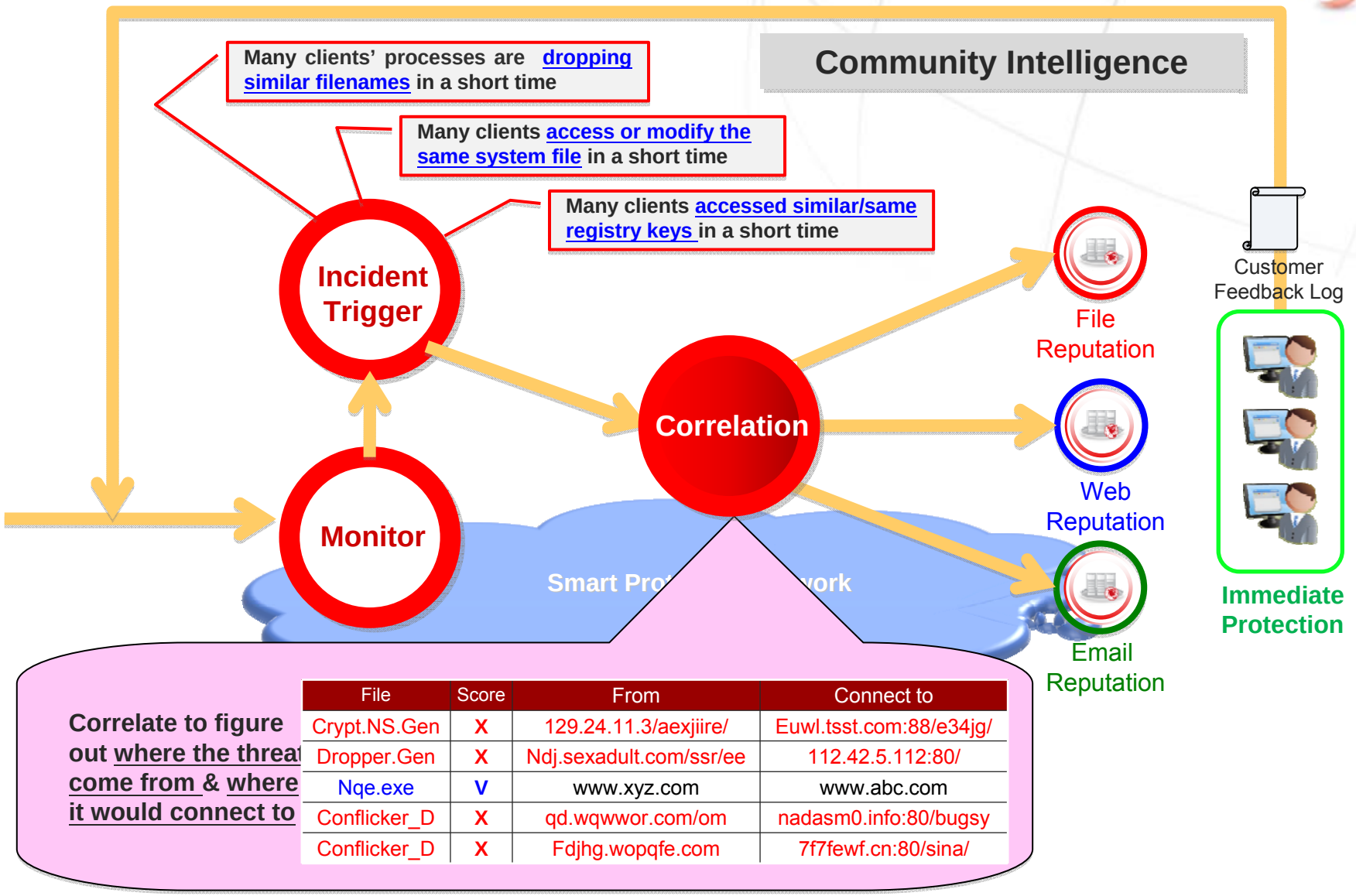


- Web Reputation
- Email Reputation
- File Reputation
- More than 1 Billion malicious websites and spam sources

Daily Traffic in the Smart Protection Network

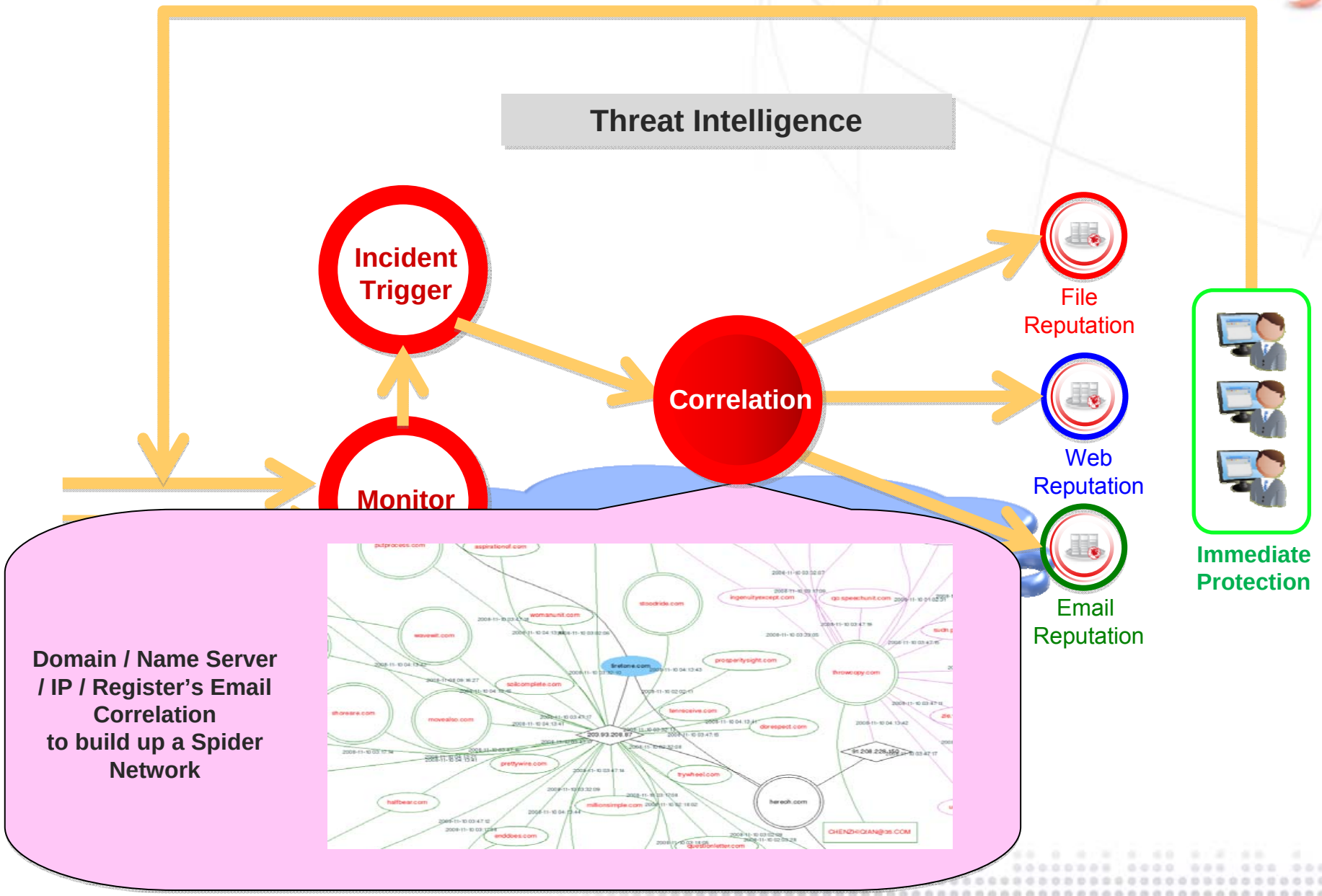


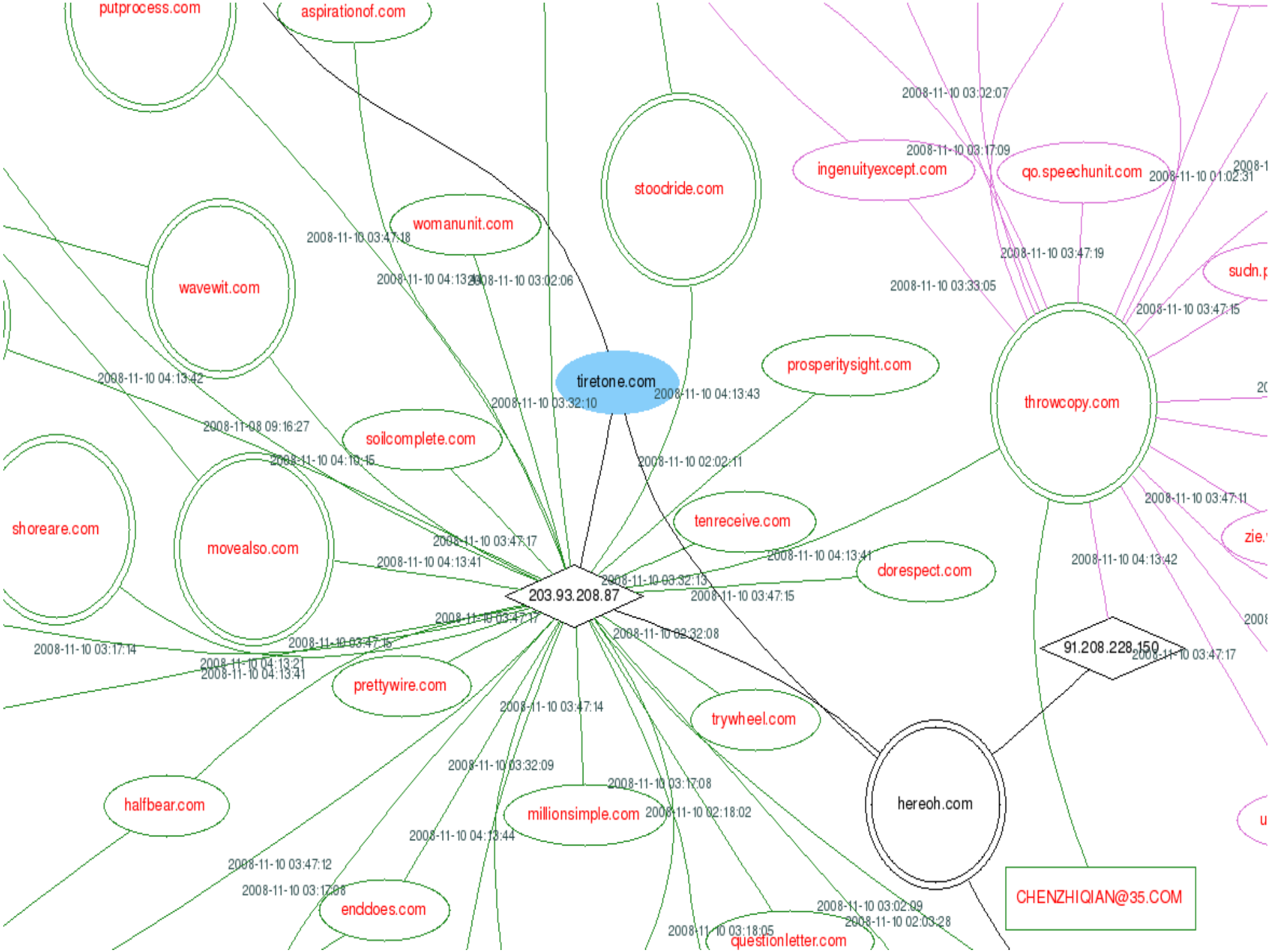
Detecting Conficker through Cloud Computing



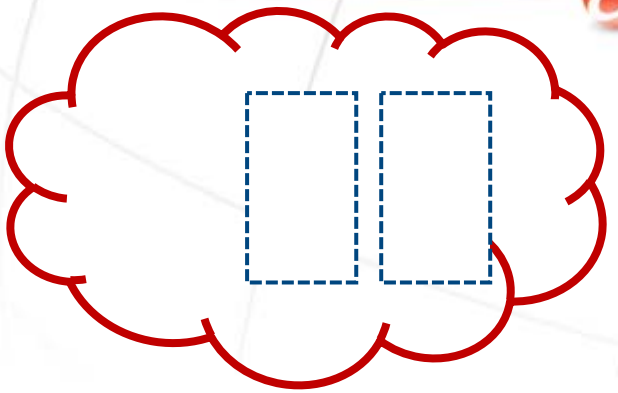
File	Score	From	Connect to
Crypt.NS.Gen	X	129.24.11.3/aexjiire/	Euwl.tsst.com:88/e34jg/
Dropper.Gen	X	Ndj.sexadult.com/ssr/ee	112.42.5.112:80/
Nqe.exe	V	www.xyz.com	www.abc.com
Conflicker_D	X	qd.wqwwor.com/om	nadasm0.info:80/bugsy
Conflicker_D	X	Fdjhg.wopqfe.com	7f7fewf.cn:80/sina/

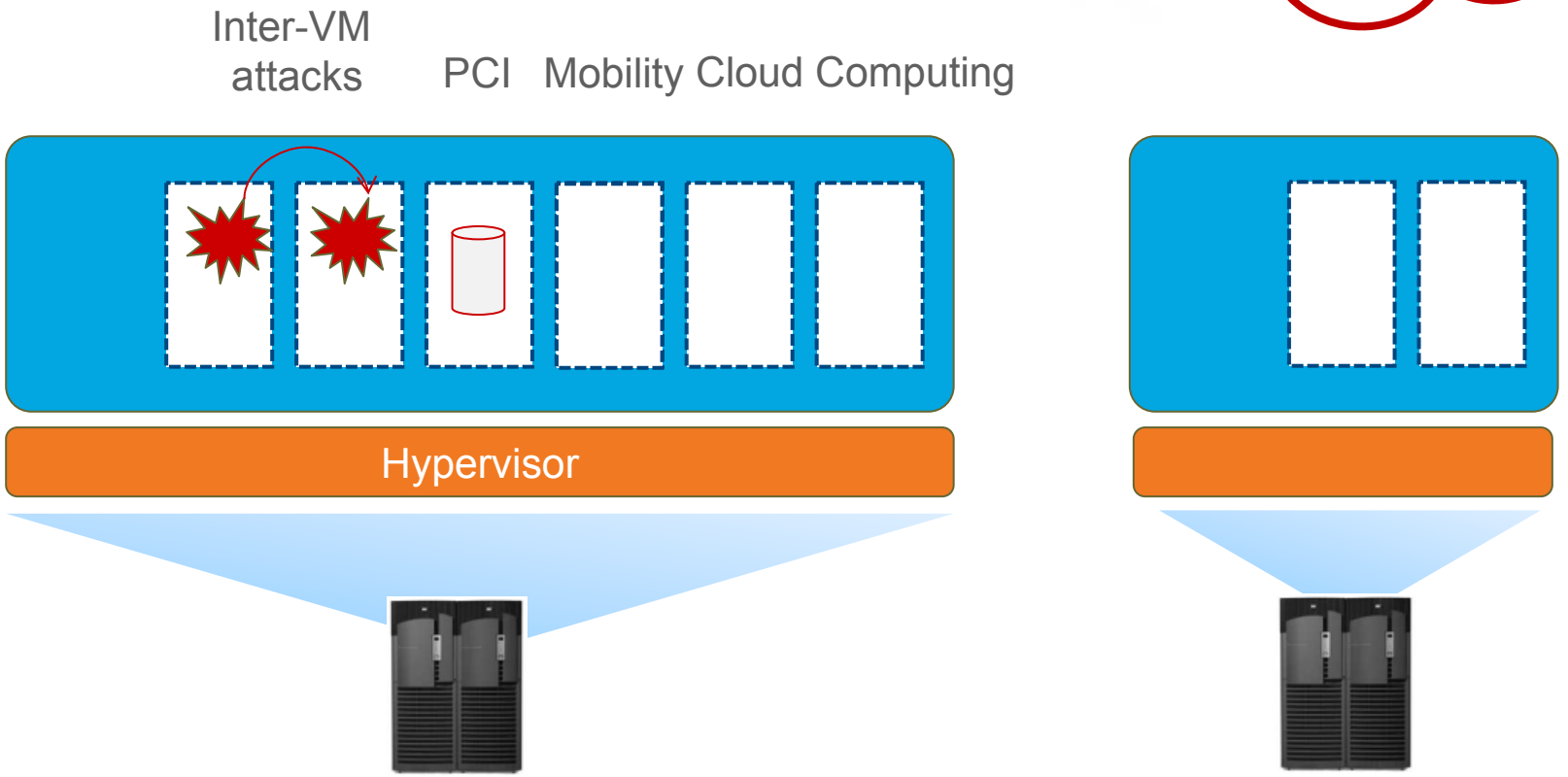
Smart Protection Network against Conficker



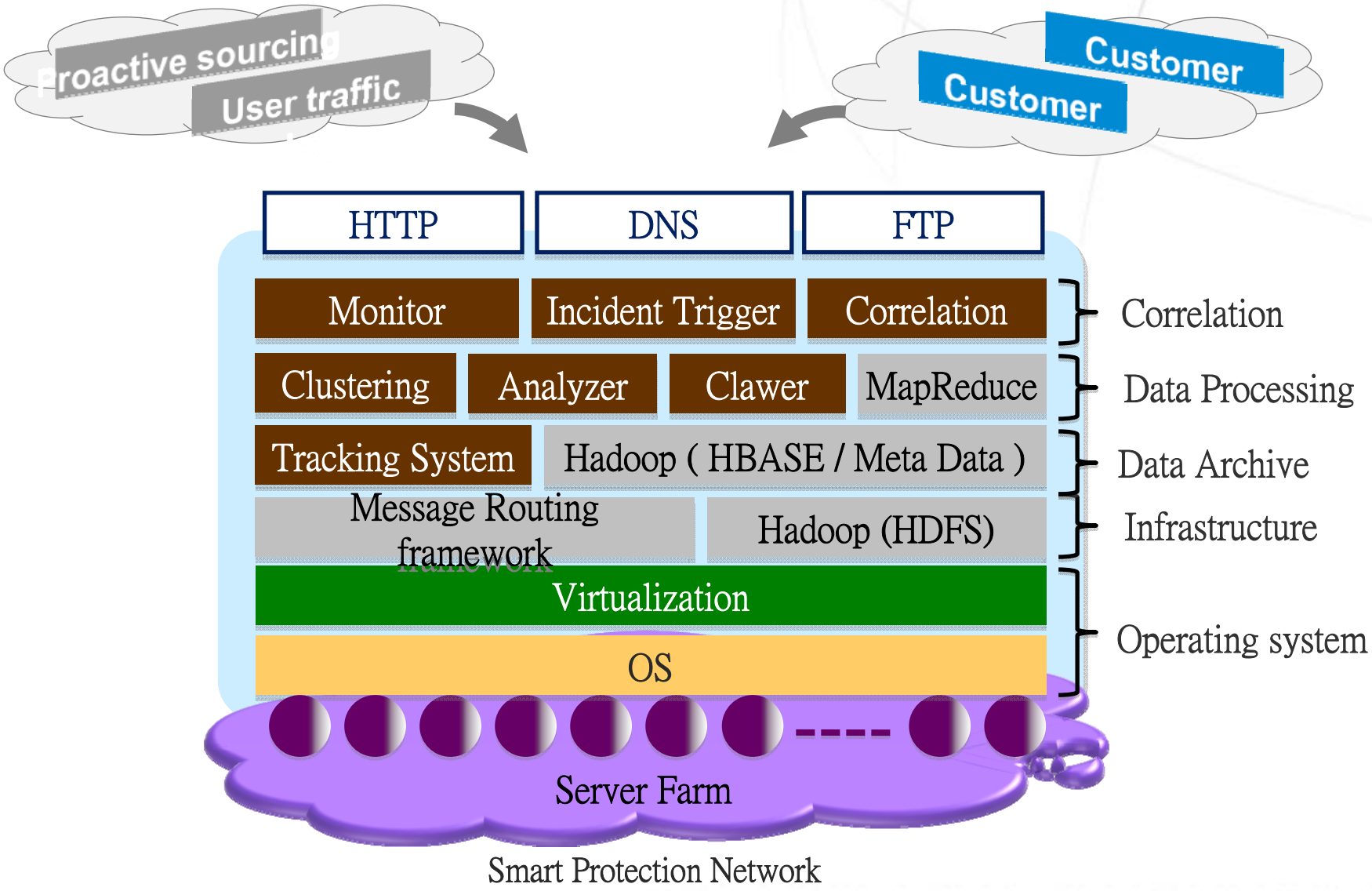

putprocess.com
aspirationof.com
stoodride.com
womanunit.com
wavewit.com
tiretone.com
prosperitysight.com
throwcopy.com
soilcomplete.com
shoreare.com
movealso.com
tenreceive.com
dorespect.com
203.93.208.87
91.208.228.150
prettywire.com
trywheel.com
halfbear.com
millionsimple.com
hereoh.com
enddoes.com
questionletter.com
ingenuityexcept.com
qo.speechunit.com
sucdn.p
zie.
CHENZHIQIAN@35.COM
2008-11-10 03:02:07
2008-11-10 03:17:09
2008-11-10 01:02:31
2008-11-10 03:47:19
2008-11-10 03:33:05
2008-11-10 03:47:15
2008-11-10 03:47:18
2008-11-10 04:13:43
2008-11-10 03:02:06
2008-11-10 04:13:42
2008-11-10 03:32:10
2008-11-10 04:13:43
2008-11-08 09:16:27
2008-11-10 04:10:15
2008-11-10 02:02:11
2008-11-10 03:47:11
2008-11-10 03:47:17
2008-11-10 04:13:41
2008-11-10 04:13:41
2008-11-10 03:32:13
2008-11-10 03:47:15
2008-11-10 04:13:42
2008-11-10 03:47:17
2008-11-10 03:47:15
2008-11-10 03:32:08
2008-11-10 03:17:14
2008-11-10 04:13:21
2008-11-10 04:13:41
2008-11-10 03:47:17
2008-11-10 03:47:14
2008-11-10 03:32:09
2008-11-10 03:17:08
2008-11-10 02:18:02
2008-11-10 04:13:44
2008-11-10 03:47:12
2008-11-10 03:17:08
2008-11-10 03:02:09
2008-11-10 02:03:28
2008-11-10 03:18:05

Cloud Computing Brings New Security Challenges

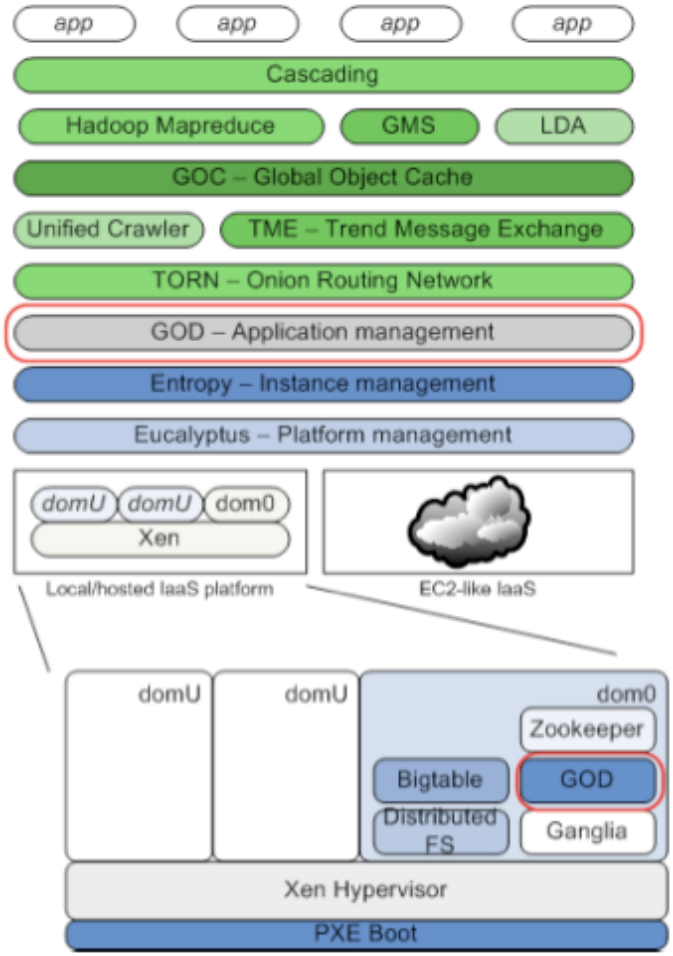




Trend Micro: Best Expertise in Cloud Computing



Avoid Lock-In by Proprietary Vendor Technology



Trend Solution Based on Open-Source Projects and Standards

Xen VM

libvirt

CloudStore

Open Nebula

KVM Hypervisor

Hadoop

GlusterFS

Eucalyptus

MapReduce

ActiveMQ

Hypertable

HBase

Ganglia

OSSEC

Nagios

amazon web services

Windows Azure

force.com

Trend of Development

2006 …

amazon.com. ⇨ amazon web services™

2007 …

Google ⇨ Google AppEngine

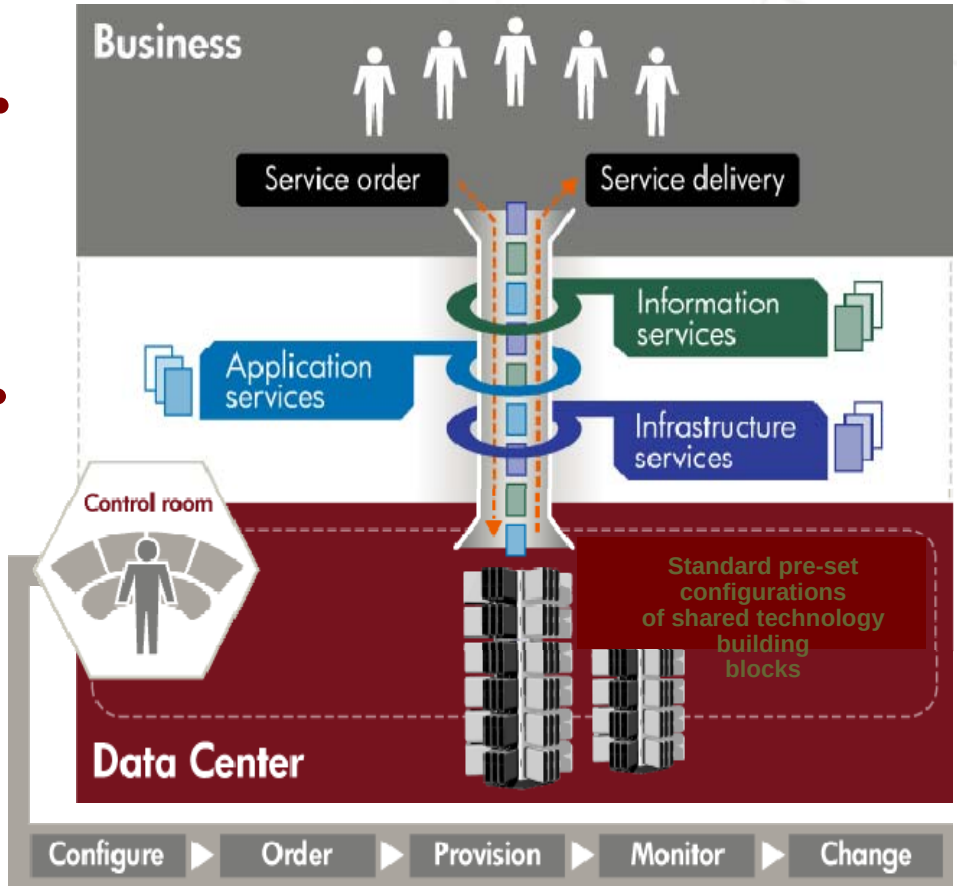
2009 …

TREND MICRO ⇨

Delivering a Service-Ready Infrastructure

Pooling and sharing of technology resources to ensure supply readily meets business demand

- **Seamless availability of business services**
- **Rapid deployment of business services**
- **Dynamic, automated infrastructure management**

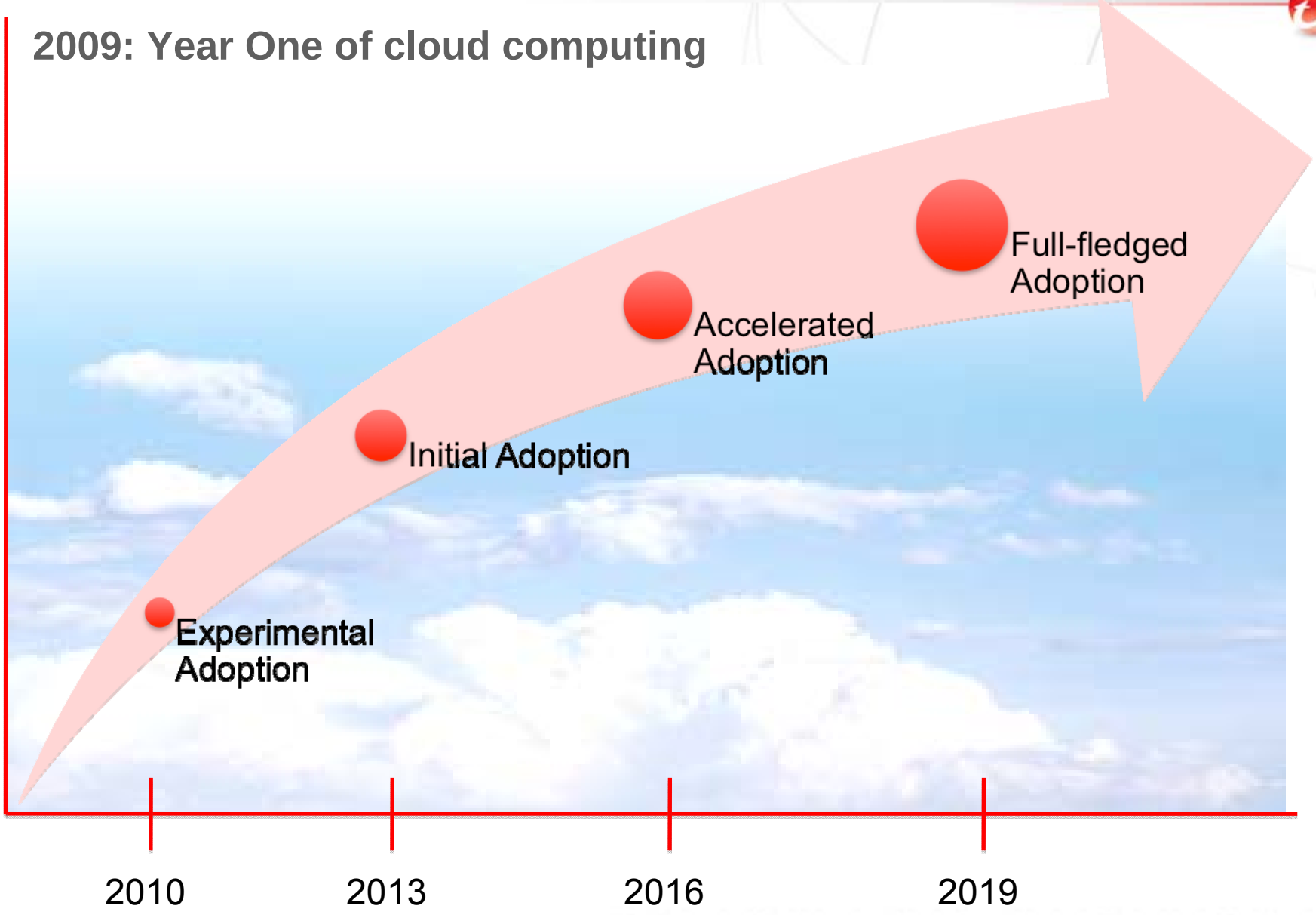


The World Is Moving Toward Cloud Computing

Eventually Everything Will Be in the Cloud

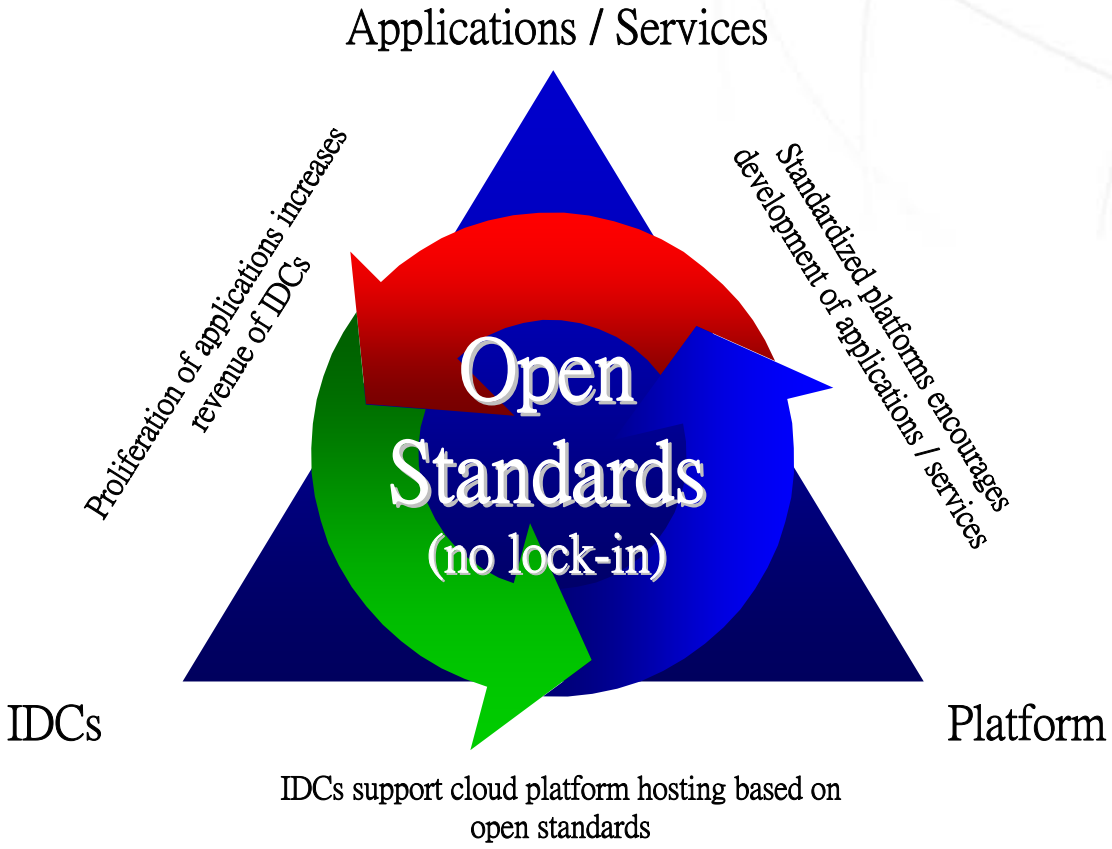
- Internet cloud as the ubiquitous source of information
- As all data storage and all computing happens in the cloud
- One can access the information from anywhere at anytime through any device
- Security in the clouds will become an issue of national security

Cloud Computing – Development Timeline



Building the Cloud Lego Blocks

Self-Reinforcing Eco-system for Cloud Computing



An Opportunity or a Threat?

TREND MICRO™

Securing Your Web World

Thank You