Missing Gap in Network Security
网络安全缺口

演讲人：Tony Teo 张泰兴

职务：Arbor Networks亚太区技术总监

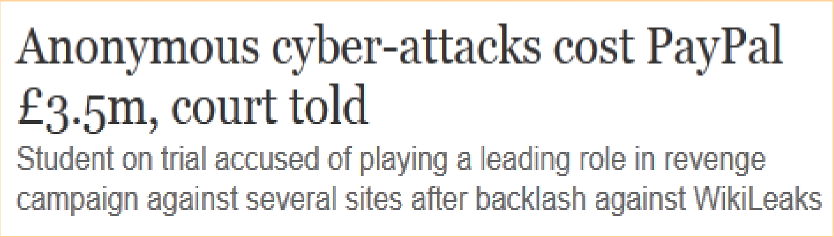
日期：25 Sept., 2014

ISC 2014 中国互联网安全大会

360互联网安全中心

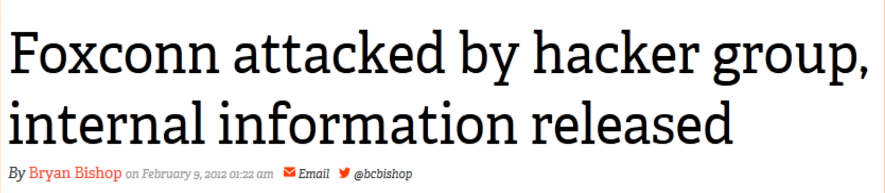
China Internet Security Conference 2014
2014中国互联网安全大会

Recent Attack Cases



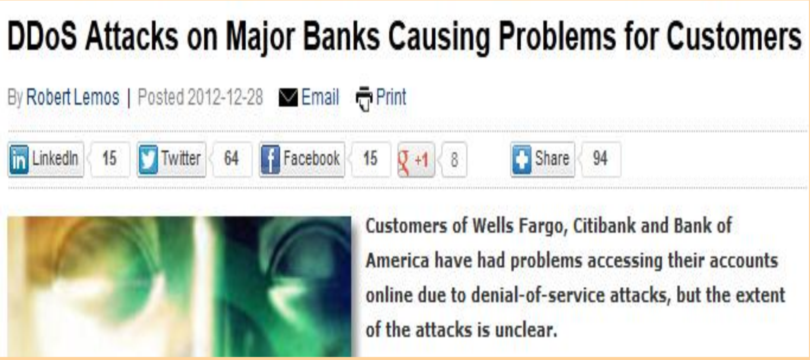
Anonymous cyber-attacks cost PayPal £3.5m, court told

Student on trial accused of playing a leading role in revenge campaign against several sites after backlash against WikiLeaks



Foxconn attacked by hacker group, internal information released

By Bryan Bishop on February 9, 2012 01:22 am Email @bcbishop

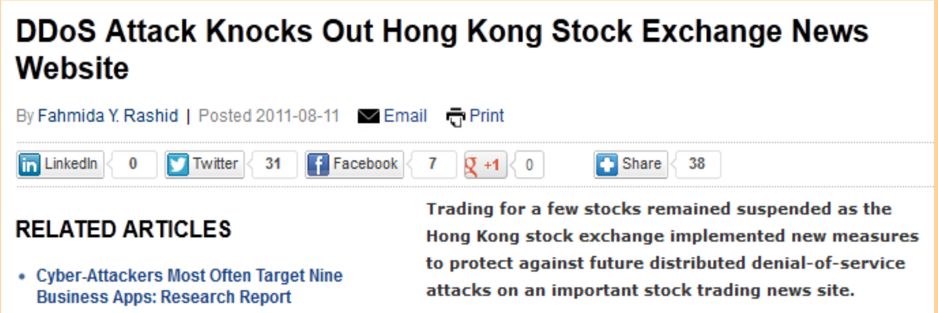


DDoS Attacks on Major Banks Causing Problems for Customers

By Robert Lemos | Posted 2012-12-28 Email Print

LinkedIn 15 Twitter 64 Facebook 15 +1 8 Share 94

Customers of Wells Fargo, Citibank and Bank of America have had problems accessing their accounts online due to denial-of-service attacks, but the extent of the attacks is unclear.



DDoS Attack Knocks Out Hong Kong Stock Exchange News Website

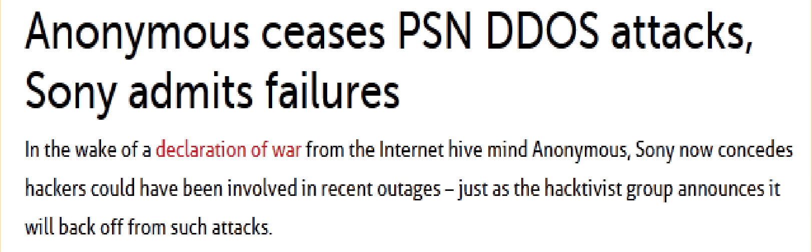
By Fahmida Y. Rashid | Posted 2011-08-11 Email Print

LinkedIn 0 Twitter 31 Facebook 7 +1 0 Share 38

RELATED ARTICLES

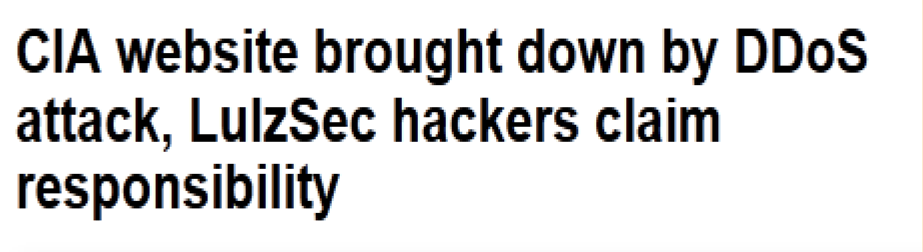
- Cyber-Attackers Most Often Target Nine Business Apps: Research Report

Trading for a few stocks remained suspended as the Hong Kong stock exchange implemented new measures to protect against future distributed denial-of-service attacks on an important stock trading news site.



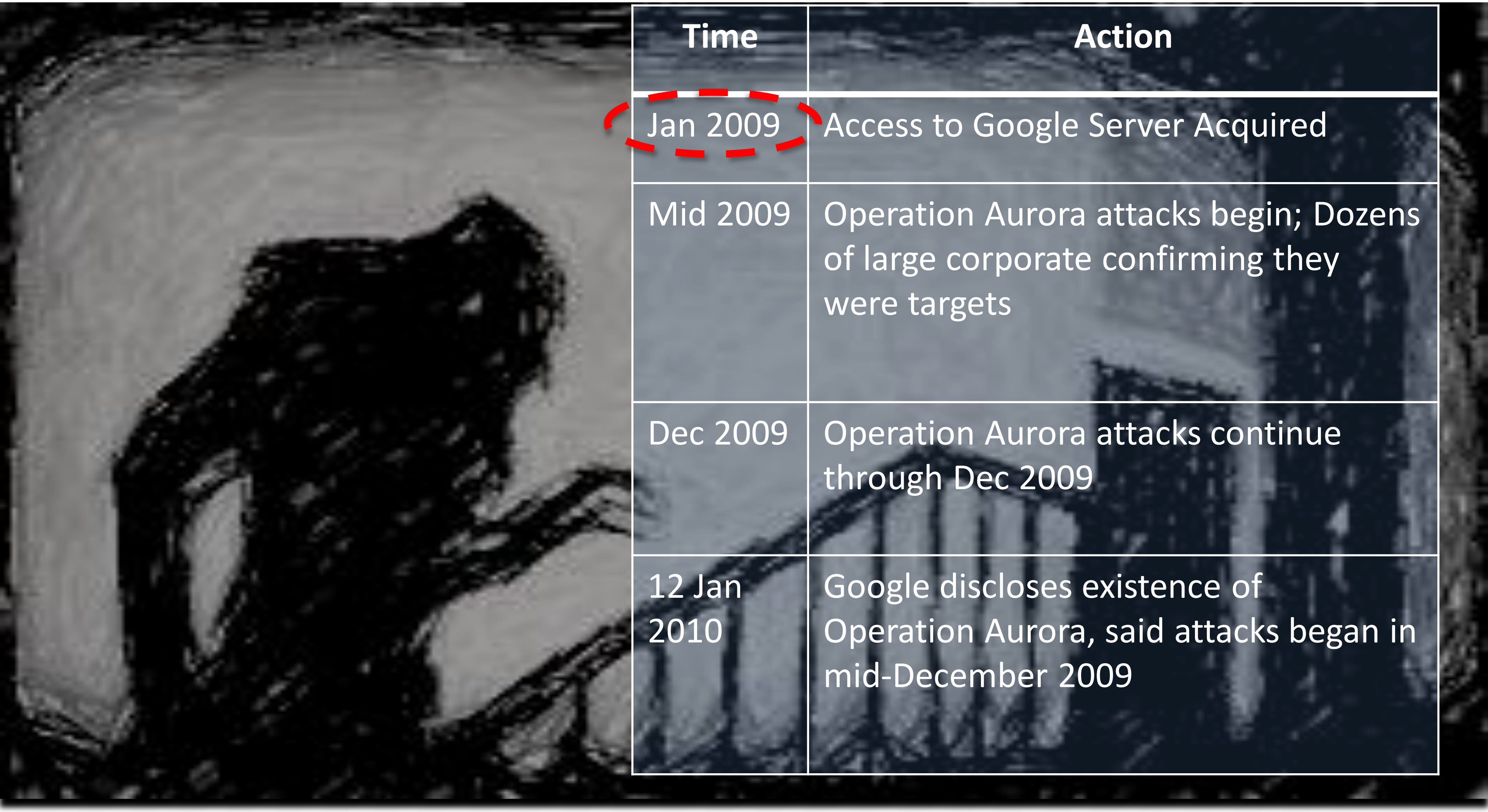
Anonymous ceases PSN DDOS attacks, Sony admits failures

In the wake of a declaration of war from the Internet hive mind Anonymous, Sony now concedes hackers could have been involved in recent outages – just as the hacktivist group announces it will back off from such attacks.



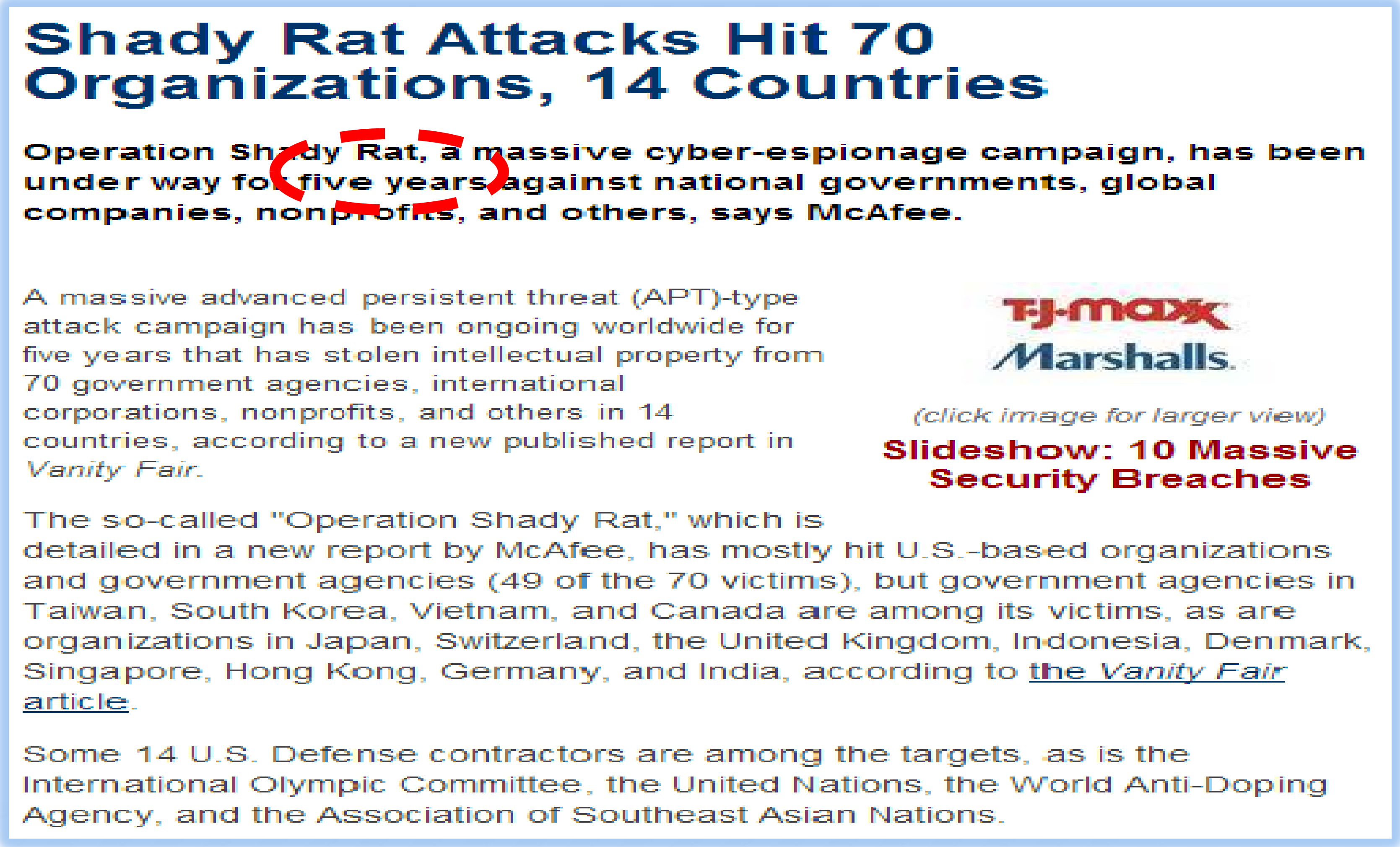
CIA website brought down by DDoS attack, LulzSec hackers claim responsibility

Operation Aurora - Timeline



Time	Action
Jan 2009	Access to Google Server Acquired
Mid 2009	Operation Aurora attacks begin; Dozens of large corporate confirming they were targets
Dec 2009	Operation Aurora attacks continue through Dec 2009
12 Jan 2010	Google discloses existence of Operation Aurora, said attacks began in mid-December 2009

APT Operation – Long Term Objective



Shady Rat Attacks Hit 70 Organizations, 14 Countries

Operation Shady Rat, a massive cyber-espionage campaign, has been under way for five years against national governments, global companies, nonprofits, and others, says McAfee.

A massive advanced persistent threat (APT)-type attack campaign has been ongoing worldwide for five years that has stolen intellectual property from 70 government agencies, international corporations, nonprofits, and others in 14 countries, according to a new published report in *Vanity Fair*.

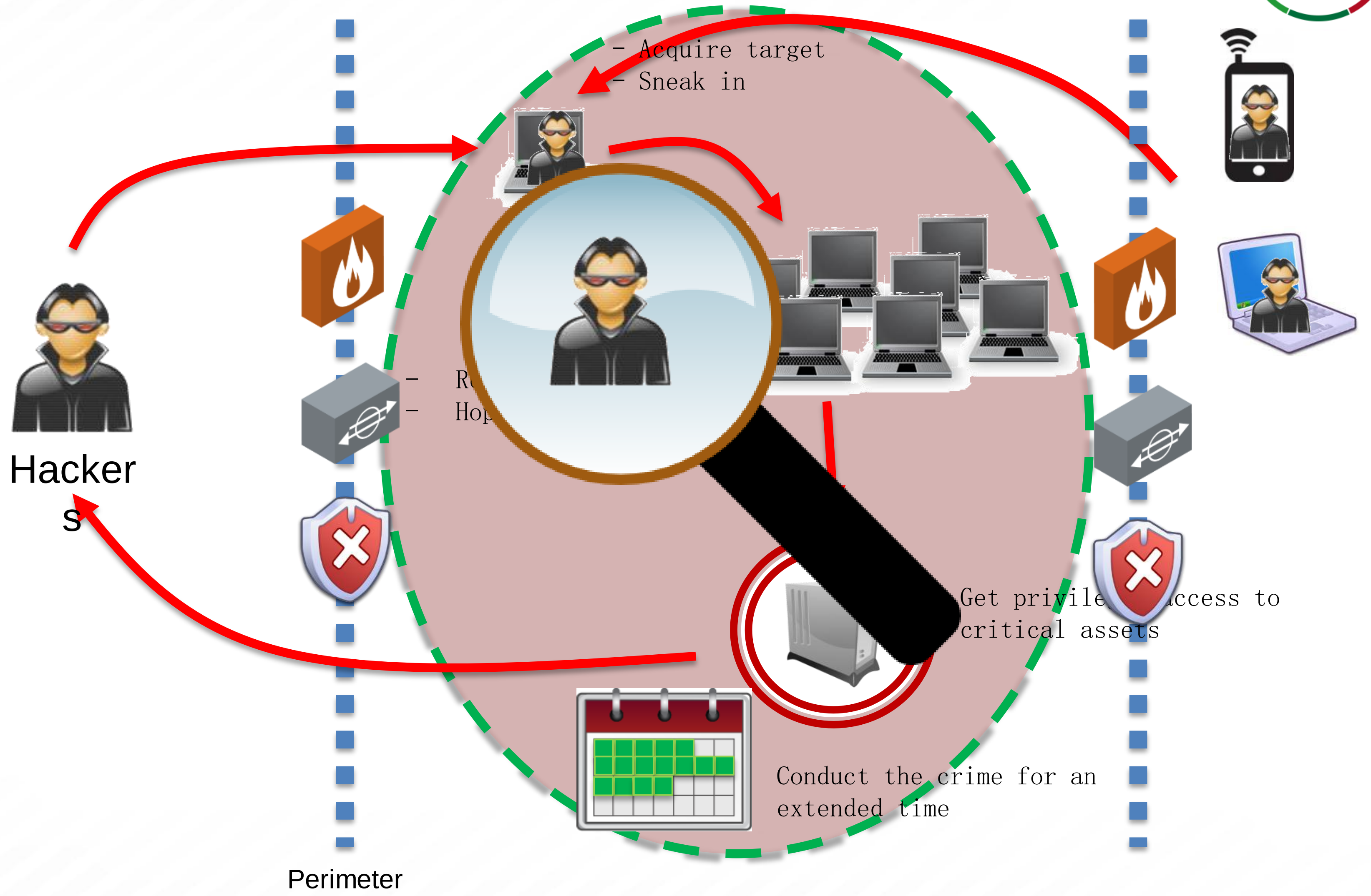
(click image for larger view)

Slideshow: 10 Massive Security Breaches

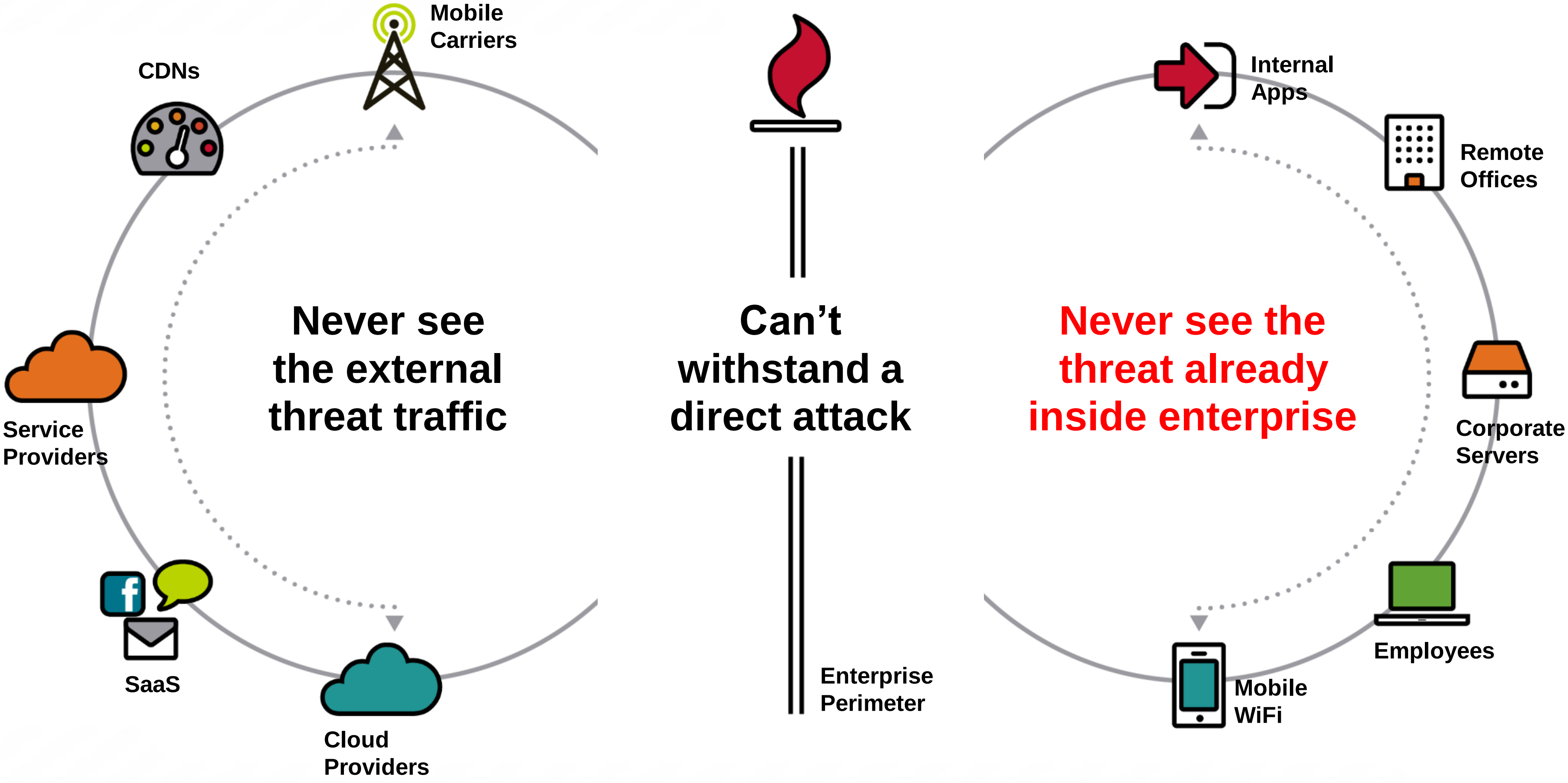
The so-called "Operation Shady Rat," which is detailed in a new report by McAfee, has mostly hit U.S.-based organizations and government agencies (49 of the 70 victims), but government agencies in Taiwan, South Korea, Vietnam, and Canada are among its victims, as are organizations in Japan, Switzerland, the United Kingdom, Indonesia, Denmark, Singapore, Hong Kong, Germany, and India, according to the *Vanity Fair* article.

Some 14 U.S. Defense contractors are among the targets, as is the International Olympic Committee, the United Nations, the World Anti-Doping Agency, and the Association of Southeast Asian Nations.

Where is the missing GAP ?


- Acquire target
- Sneak in
- R
- Hop
Get privile access to critical assets
Conduct the crime for an extended time
Hacker s
Perimeter

Existing Solutions Have Critical Gaps



Never see the external threat traffic

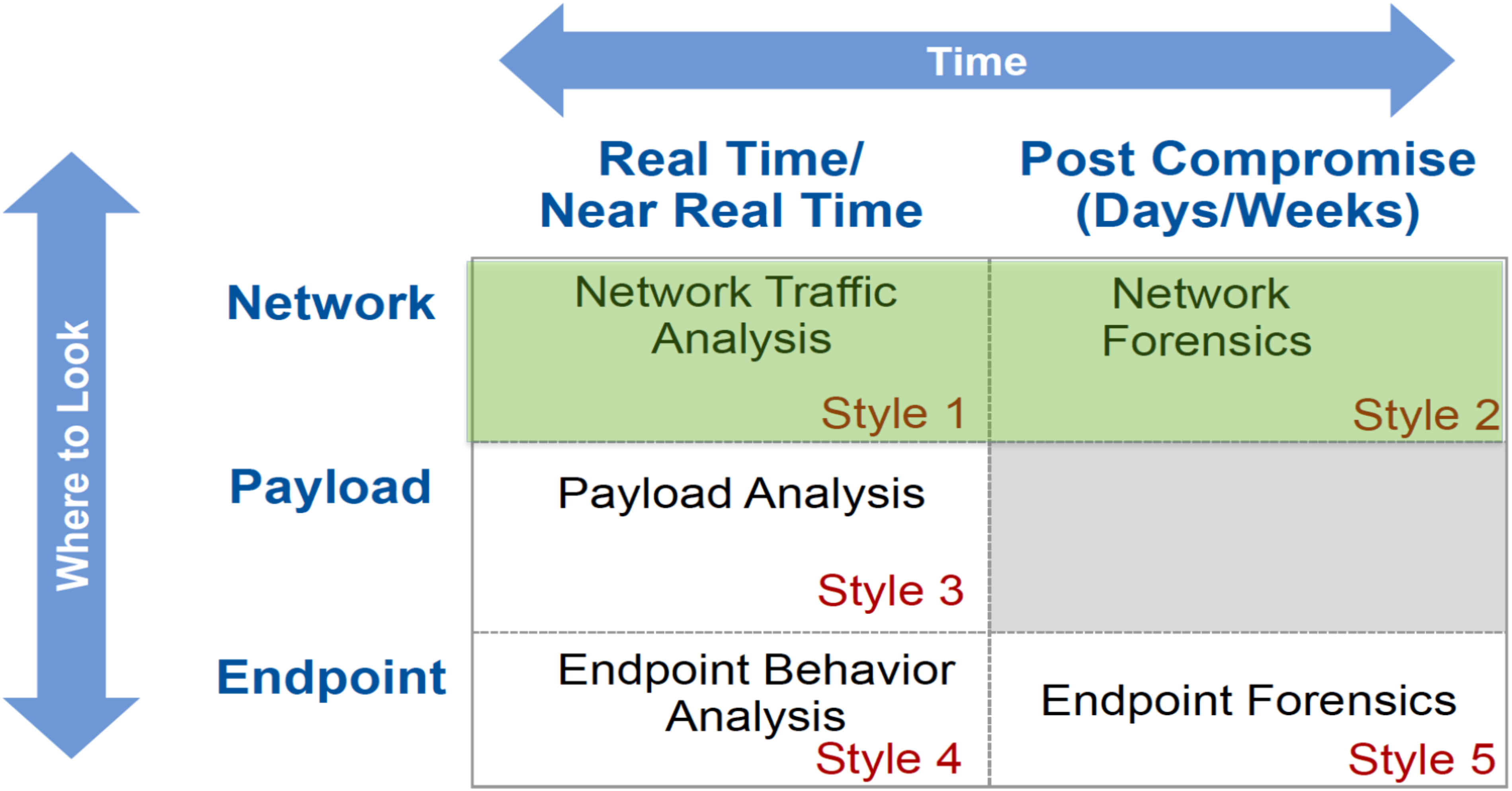
Can’t withstand a direct attack

Never see the threat already inside enterprise

ISC 2014

Pravail Network Security Intelligent

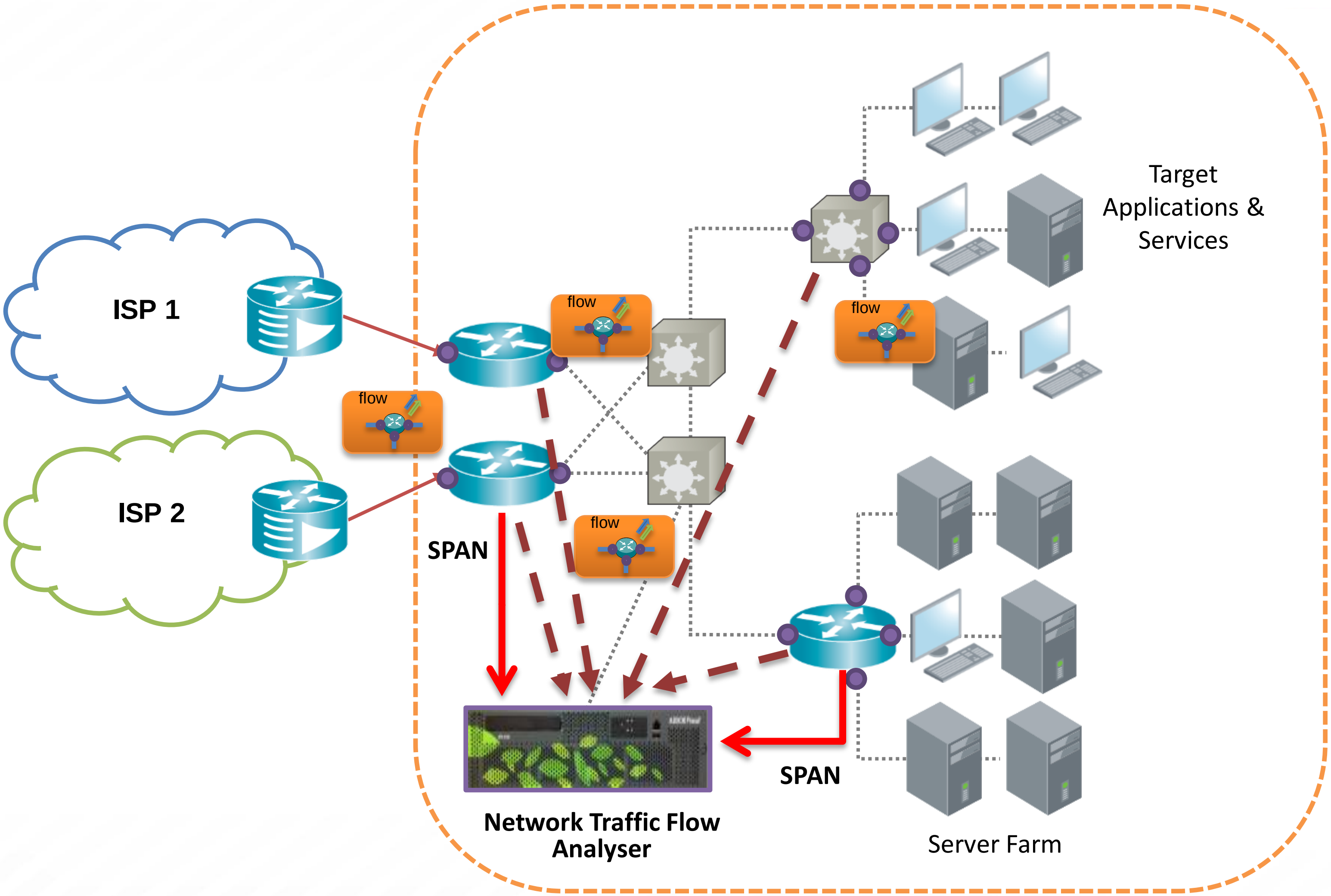
Five Styles of Advanced Threat Defense



	Real Time/ Near Real Time	Post Compromise (Days/Weeks)
Network	Network Traffic Analysis Style 1	Network Forensics Style 2
Payload	Payload Analysis Style 3	
Endpoint	Endpoint Behavior Analysis Style 4	Endpoint Forensics Style 5

Source：Gartner - **Five Styles of Advanced**

Style 1 : Network Traffic Analysis



NSI- Enterprise-Wide Visibility

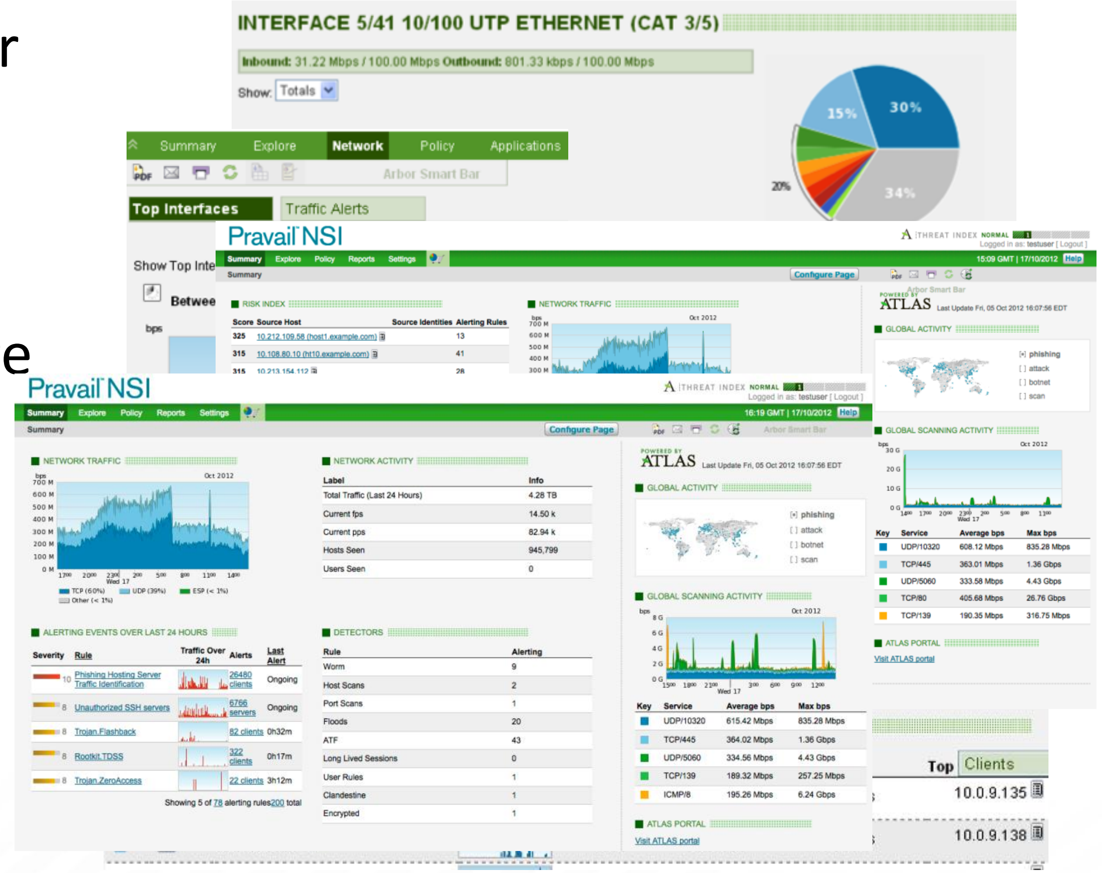
ISC 2014

The Enterprise Visibility Needed To Secure the Network
“You Simply Can’t Secure It if You Can’t See It”

Detect who is accessing your network, when and what they are doing.

Analyze where your risks are and how to stop them.

Address problems, armed with context and security intelligence



INTERFACE 5/41 10/100 UTP ETHERNET (CAT 3/5)

Inbound: 31.22 Mbps / 100.00 Mbps Outbound: 801.33 kbps / 100.00 Mbps

Show: Totals

Pravail NSI — THREAT INDEX NORMAL 1 — Logged in as: testuser [Logout] — 15:09 GMT | 17/10/2012 Help

RISK INDEX

Score	Source Host	Source Identities	Alerting Rules
325	10.212.109.58 (host1.example.com)		13
315	10.108.80.10 (ht10.example.com)		41
315	10.213.154.112		28

NETWORK TRAFFIC

POWERED BY ATLAS Last Update Fri, 05 Oct 2012 16:07:56 EDT

GLOBAL ACTIVITY

[•] phishing
[ ] attack
[ ] botnet
[ ] scan

GLOBAL SCANNING ACTIVITY

Key	Service	Average bps	Max bps
🟦	UDP/10320	608.12 Mbps	835.28 Mbps
🟦	TCP/445	363.01 Mbps	1.36 Gbps
🟩	UDP/5060	333.58 Mbps	4.43 Gbps
🟩	TCP/80	405.68 Mbps	26.76 Gbps
🟧	TCP/139	190.35 Mbps	316.75 Mbps

ATLAS PORTAL

Visit ATLAS portal

Top Clients

10.0.9.135
10.0.9.138

Pravail NSI — THREAT INDEX NORMAL 1 — Logged in as: testuser [Logout] — 16:19 GMT | 17/10/2012 Help

NETWORK TRAFFIC

NETWORK ACTIVITY

Label	Info
Total Traffic (Last 24 Hours)	4.28 TB
Current fps	14.50 k
Current pps	82.94 k
Hosts Seen	945,799
Users Seen	0

ALERTING EVENTS OVER LAST 24 HOURS

Severity	Rule	Traffic Over 24h	Alerts	Last Alert
10	Phishing Hosting Server Traffic Identification		26480 clients	Ongoing
8	Unauthorized SSH servers		6766 servers	Ongoing
8	Trojan.Flashback		82 clients	0h32m
8	Rootkit.TDSS		322 clients	0h17m
8	Trojan.ZeroAccess		22 clients	3h12m

Showing 5 of 78 alerting rules200 total

DETECTORS

Rule	Alerting
Worm	9
Host Scans	2
Port Scans	1
Floods	20
ATF	43
Long Lived Sessions	0
User Rules	1
Clandestine	1
Encrypted	1

POWERED BY ATLAS Last Update Fri, 05 Oct 2012 16:07:56 EDT

GLOBAL ACTIVITY

[•] phishing
[ ] attack
[ ] botnet
[ ] scan

GLOBAL SCANNING ACTIVITY

Key	Service	Average bps	Max bps
🟦	UDP/10320	615.42 Mbps	835.28 Mbps
🟦	TCP/445	364.02 Mbps	1.36 Gbps
🟩	UDP/5060	334.56 Mbps	4.43 Gbps
🟩	TCP/139	189.32 Mbps	257.25 Mbps
🟧	ICMP/8	195.26 Mbps	6.24 Gbps

ATLAS PORTAL

Visit ATLAS portal

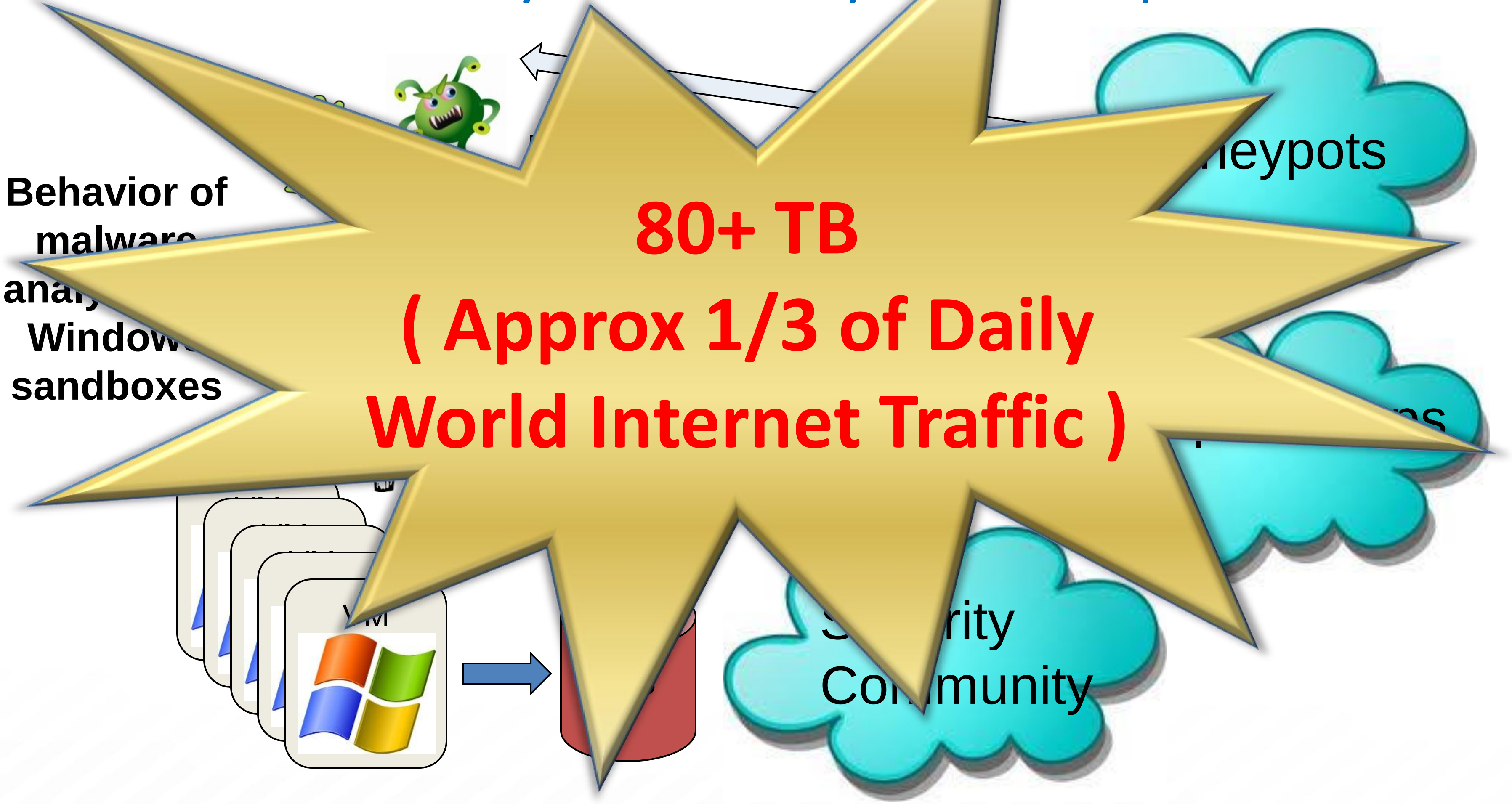
Who is Arbor Networks?

A Trusted & Proven Vendor Securing the World's Largest and Most Demanding Networks

90%	Percentage of world's Tier 1 service providers who are Arbor customers at&t verizon BT NTT 中国电信 CHINA TELECOM TATA vodafone Telefonica T-Com france telecom
105	Number of countries with Arbor products deployed
80+ Tbps	Amount of global traffic monitored by the ATLAS security intelligence initiative right now – ***30% of global Internet traffic!***
#1	Arbor market position in Carrier, Enterprise and Mobile DDoS equipment market segments – 61% of total market [Infonetics Research Dec 2011]
14	Number of years Arbor has been delivering innovative security and network visibility technologies & products

ASERT Malware Analysis Infrastructure

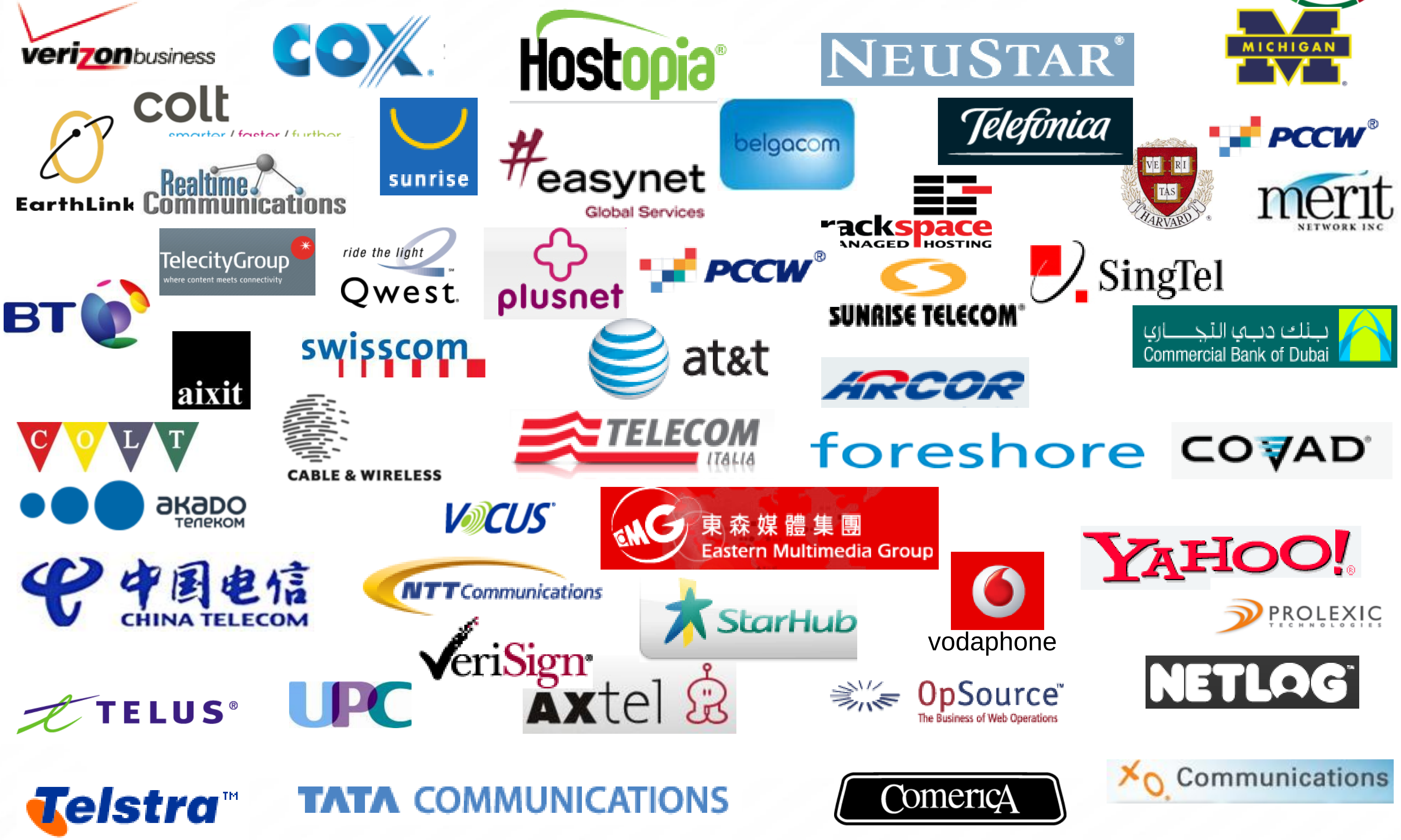
Automated bulk dynamic analysis f samples



80+ TB

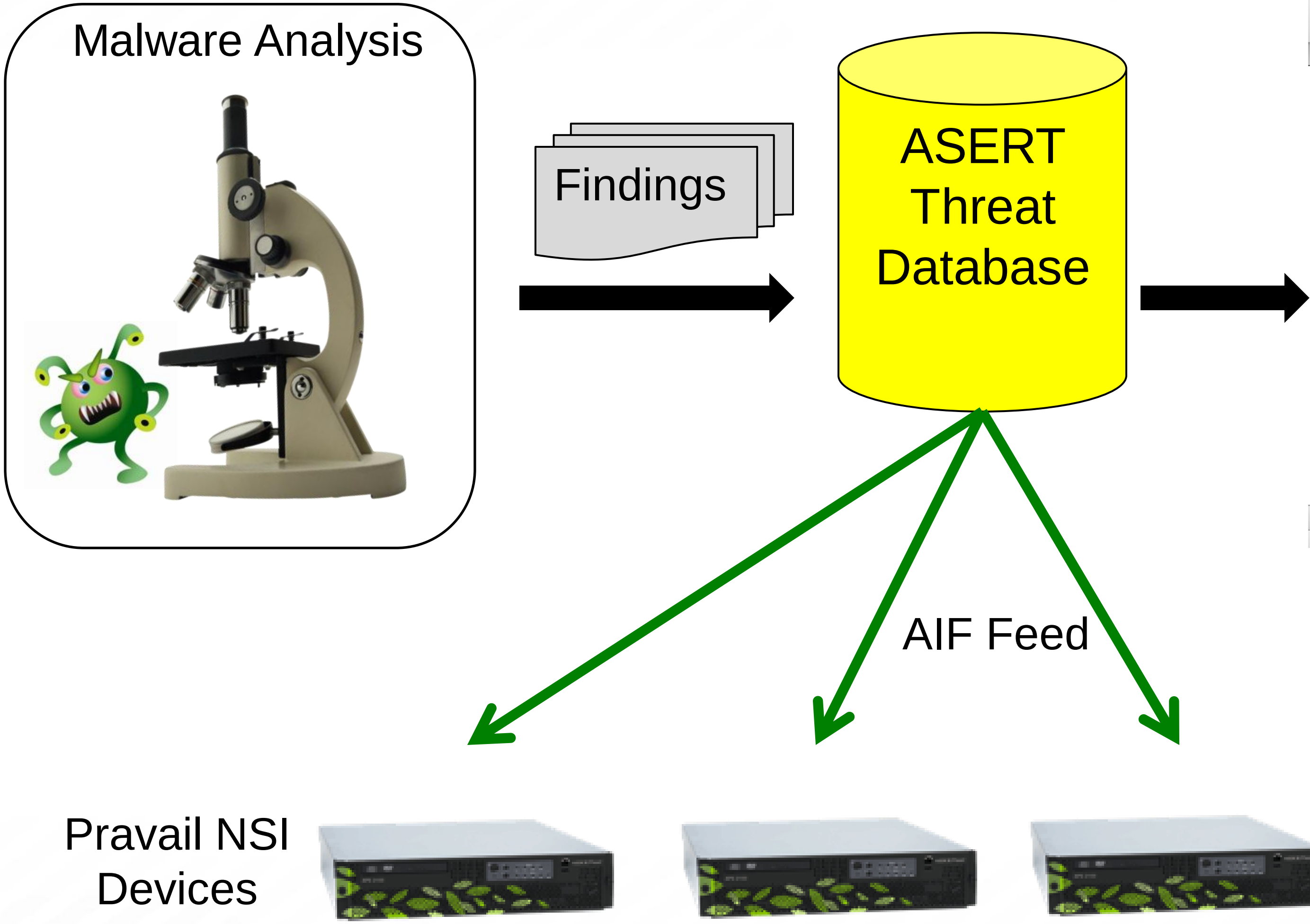
(Approx 1/3 of Daily World Internet Traffic)

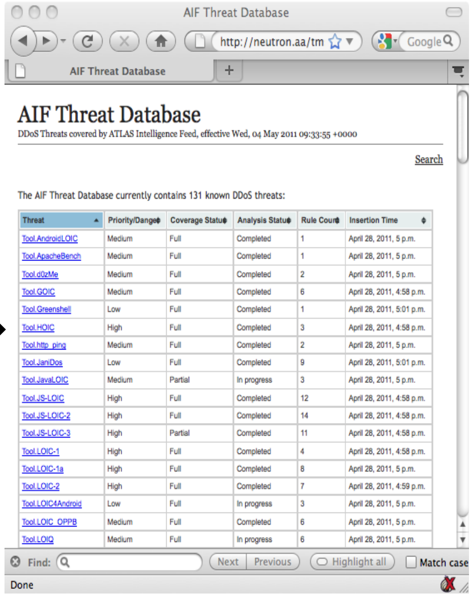
Sampling of Arbor's Customers



* These customers have given Arbor Networks authorization to use their names publicly. Over

Pravail AIF Security Intelligent





AIF Threat Database

DDoS Threats covered by ATLAS Intelligence Feed, effective Wed, 04 May 2011 09:33:55 +0000

Search

The AIF Threat Database currently contains 131 known DDoS threats:

Threat	Priority/Dange	Coverage Statu	Analysis Statu	Rule Coun	Insertion Time
Tool.AndroidLOIC	Medium	Full	Completed	1	April 28, 2011, 5 p.m.
Tool.ApacheBench	Medium	Full	Completed	1	April 28, 2011, 5 p.m.
Tool.d0zMe	Medium	Full	Completed	2	April 28, 2011, 5 p.m.
Tool.GOIC	Medium	Full	Completed	6	April 28, 2011, 4:58 p.m.
Tool.Greenshell	Low	Full	Completed	1	April 28, 2011, 5:01 p.m.
Tool.HOIC	High	Full	Completed	3	April 28, 2011, 4:58 p.m.
Tool.http_ping	Medium	Full	Completed	2	April 28, 2011, 5 p.m.
Tool.JaniDos	Low	Full	Completed	9	April 28, 2011, 5:01 p.m.
Tool.JavaLOIC	Medium	Partial	In progress	3	April 28, 2011, 5 p.m.
Tool.JS-LOIC	High	Full	Completed	12	April 28, 2011, 4:58 p.m.
Tool.JS-LOIC-2	High	Full	Completed	14	April 28, 2011, 4:58 p.m.
Tool.JS-LOIC-3	High	Partial	Completed	11	April 28, 2011, 4:58 p.m.
Tool.LOIC-1	High	Full	Completed	4	April 28, 2011, 4:58 p.m.
Tool.LOIC-1a	High	Full	Completed	8	April 28, 2011, 5 p.m.
Tool.LOIC-2	High	Full	Completed	7	April 28, 2011, 4:59 p.m.
Tool.LOIC4Android	Low	Full	In progress	3	April 28, 2011, 5 p.m.
Tool.LOIC_OPPB	Medium	Full	Completed	6	April 28, 2011, 5 p.m.
Tool.LOIQ	Medium	Full	In progress	6	April 28, 2011, 5 p.m.

AIF Search Interface

NSI Use Cases examples

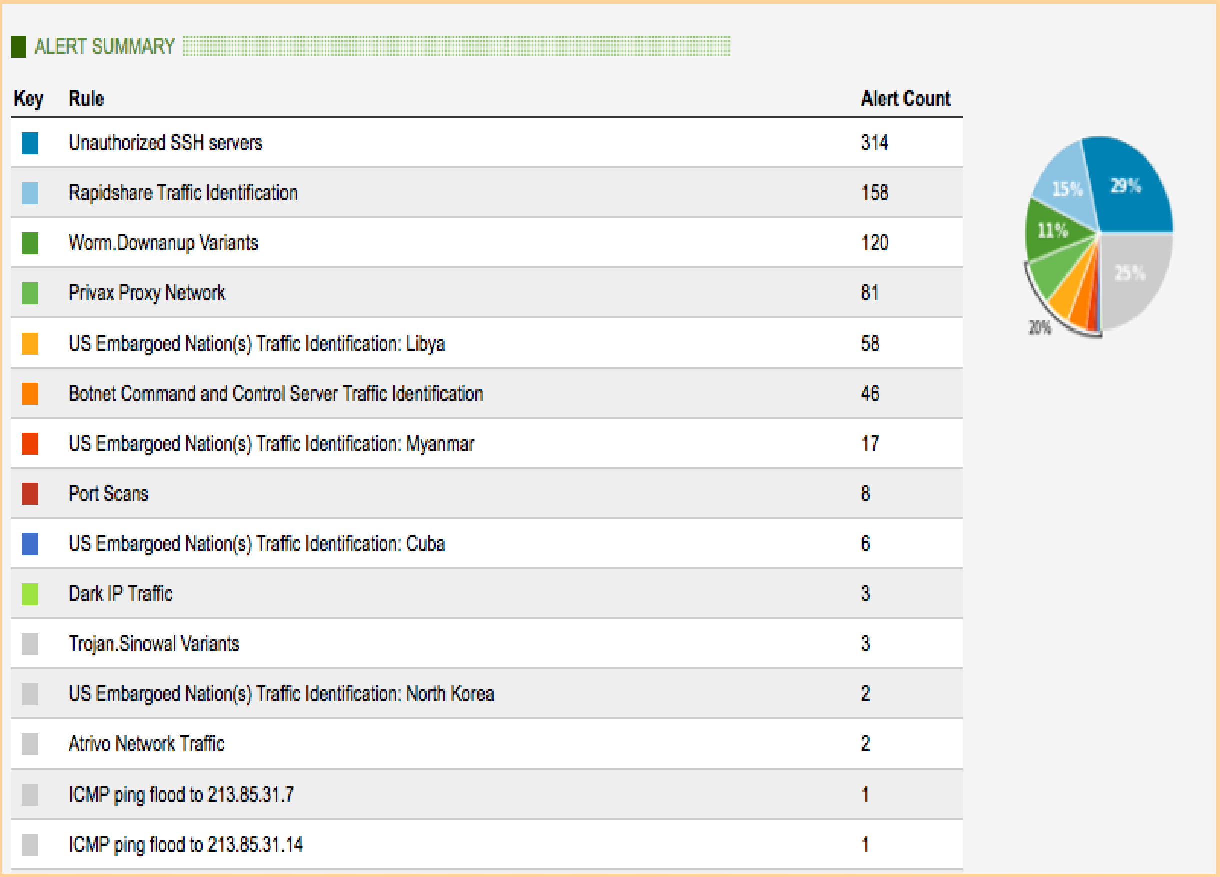
Enterprise Security Posture

NSI - Advanced Threat Detection

Pravail NSI detects and alerts diverse threats to the network from the inside

- Port and Host Scans
- Botnets
- Spyware
- Phishing Attempts
- Dark IP Detection
- Unauthorized Access
- Data Exfiltration

- New active Clients
- New active Servers
- New active Services
- New Relationships between hosts



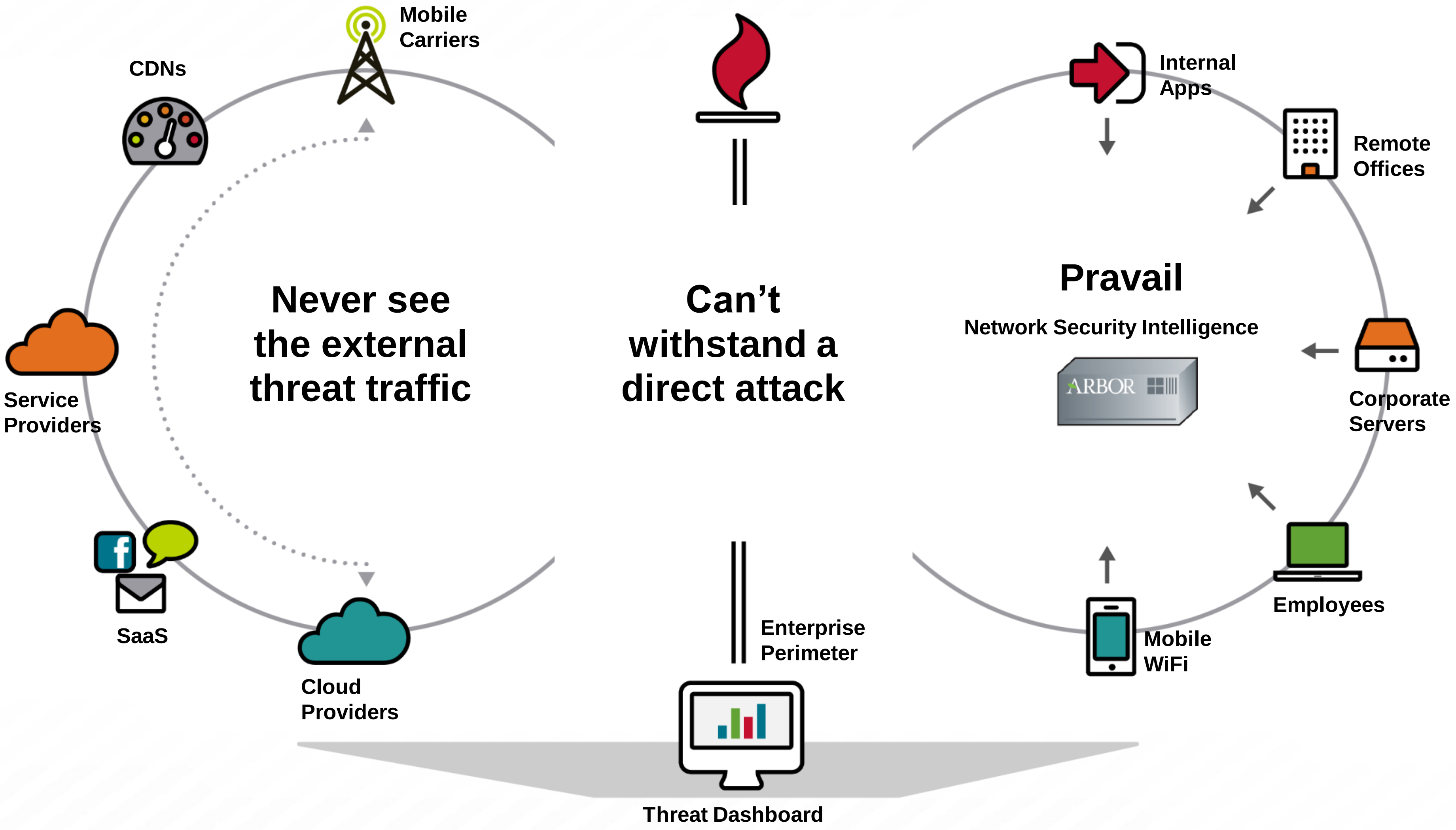
ALERT SUMMARY

Key	Rule	Alert Count
🟦	Unauthorized SSH servers	314
🟦	Rapidshare Traffic Identification	158
🟩	Worm.Downanup Variants	120
🟩	Privax Proxy Network	81
🟧	US Embargoed Nation(s) Traffic Identification: Libya	58
🟧	Botnet Command and Control Server Traffic Identification	46
🟥	US Embargoed Nation(s) Traffic Identification: Myanmar	17
🟥	Port Scans	8
🟦	US Embargoed Nation(s) Traffic Identification: Cuba	6
🟩	Dark IP Traffic	3
⬜	Trojan.Sinowal Variants	3
⬜	US Embargoed Nation(s) Traffic Identification: North Korea	2
⬜	Atrivo Network Traffic	2
⬜	ICMP ping flood to 213.85.31.7	1
⬜	ICMP ping flood to 213.85.31.14	1

NSI Use Cases examples

- Data Theft / Data Leakage Detection
- Insider Threat Detection
- Advance Threat / APT Detection
  - Phishing / Spyware Behaviors Detection
  - Malware / Zero Day Behaviors Detection
  - Botnet Behaviors Detection
  - Unauthorised access
- BYOD and Mobile Devices Behaviors Detection
- Application usage monitoring
- Compliance Reporting
- Forensic Analysis
- More……..

Arbor’s Solution Bridges the Gaps



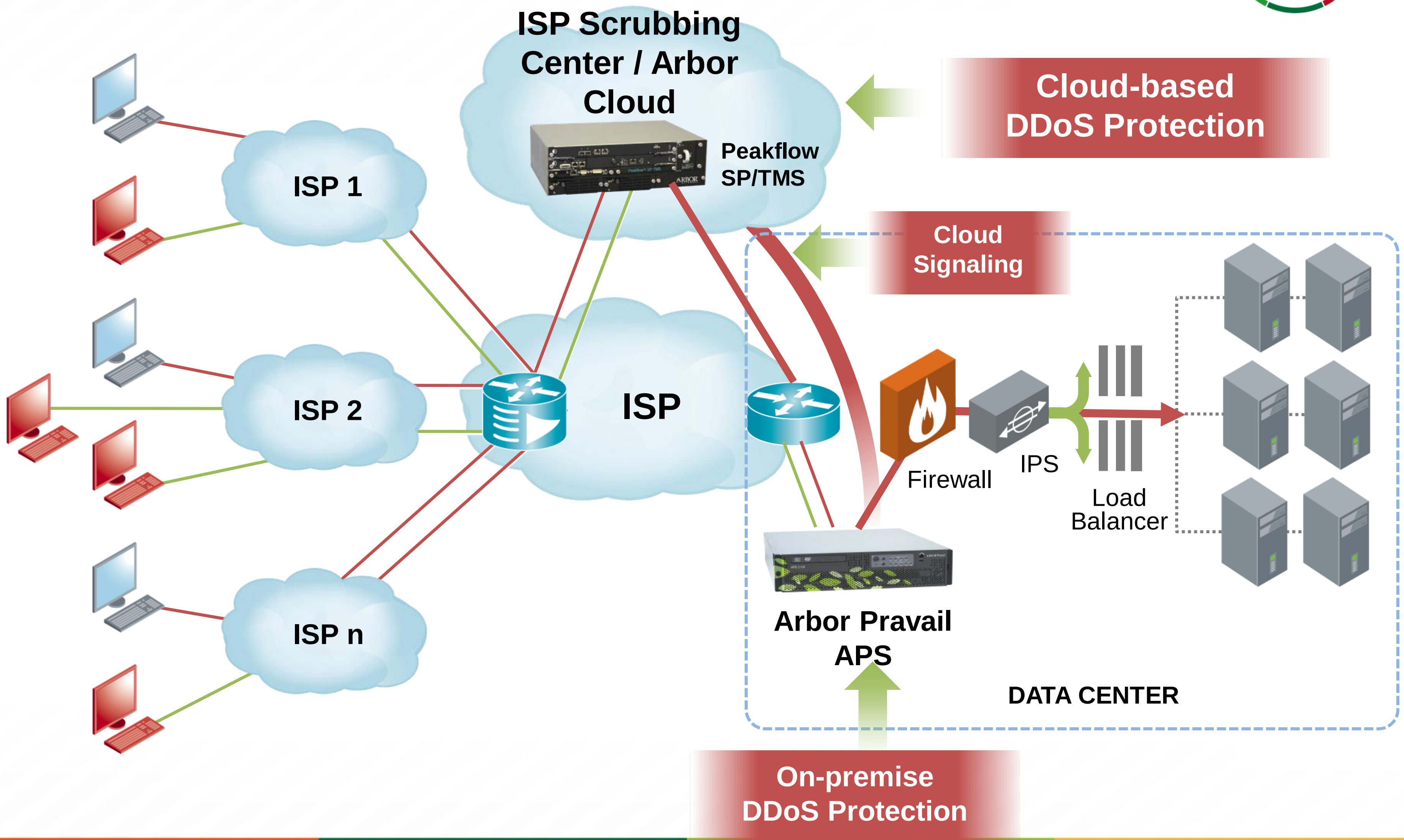
Never see the external threat traffic

Can’t withstand a direct attack

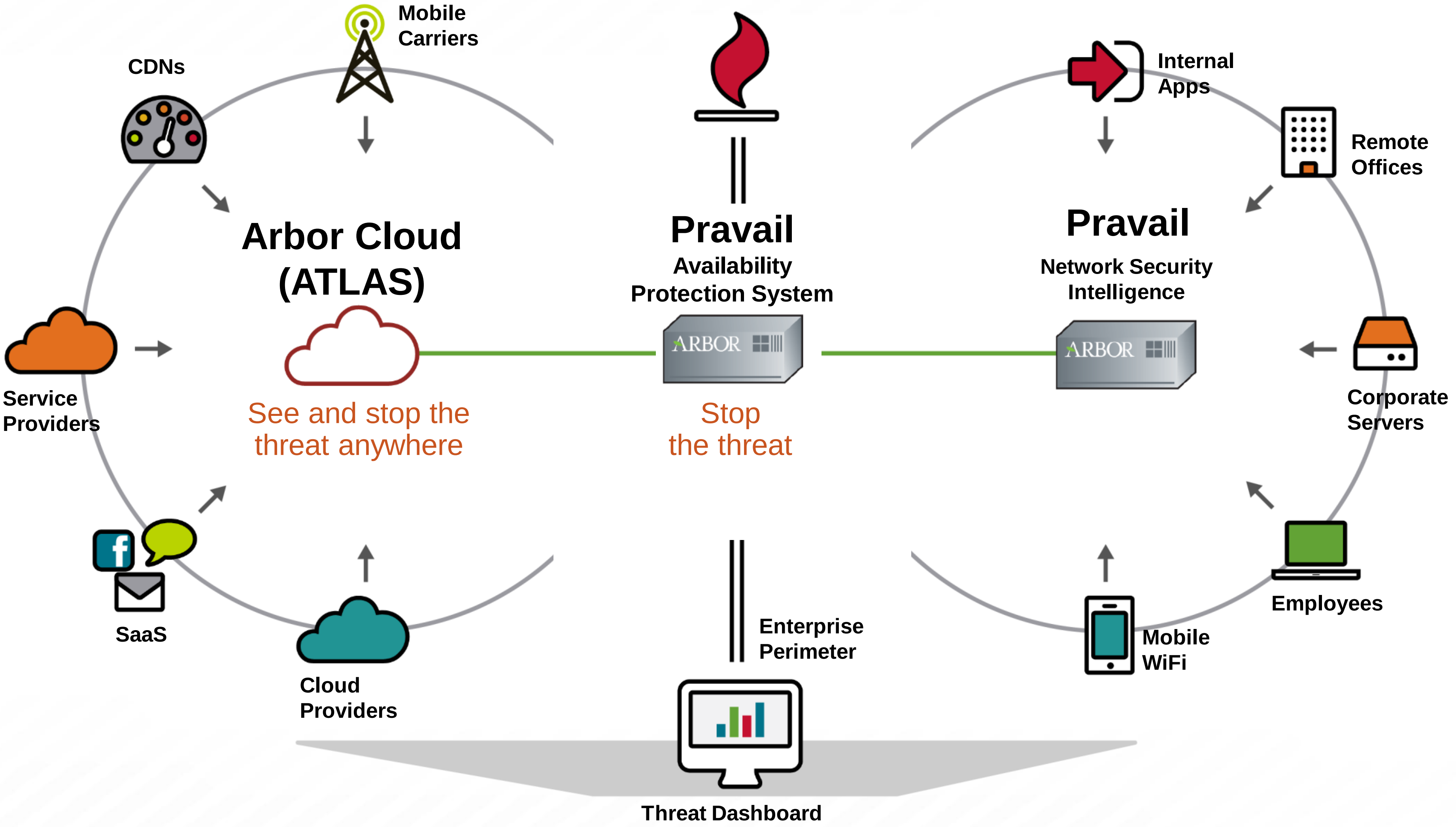
Pravail

Network Security Intelligence

Arbor’s Multi-Layer DDoS Protection



Arbor’s Solution Bridges the Gaps



Thank You !