

India
**EXECUTIVE
SUMMIT**
A FOCUS SERIES EVENT



The future of security

Michael Sentonas
VP, Chief Technology
Officer, APAC

What is the
FASTEST way
to get
PROTECTION?





The **FLOPPY**
was the **BIGGEST**
problem we had

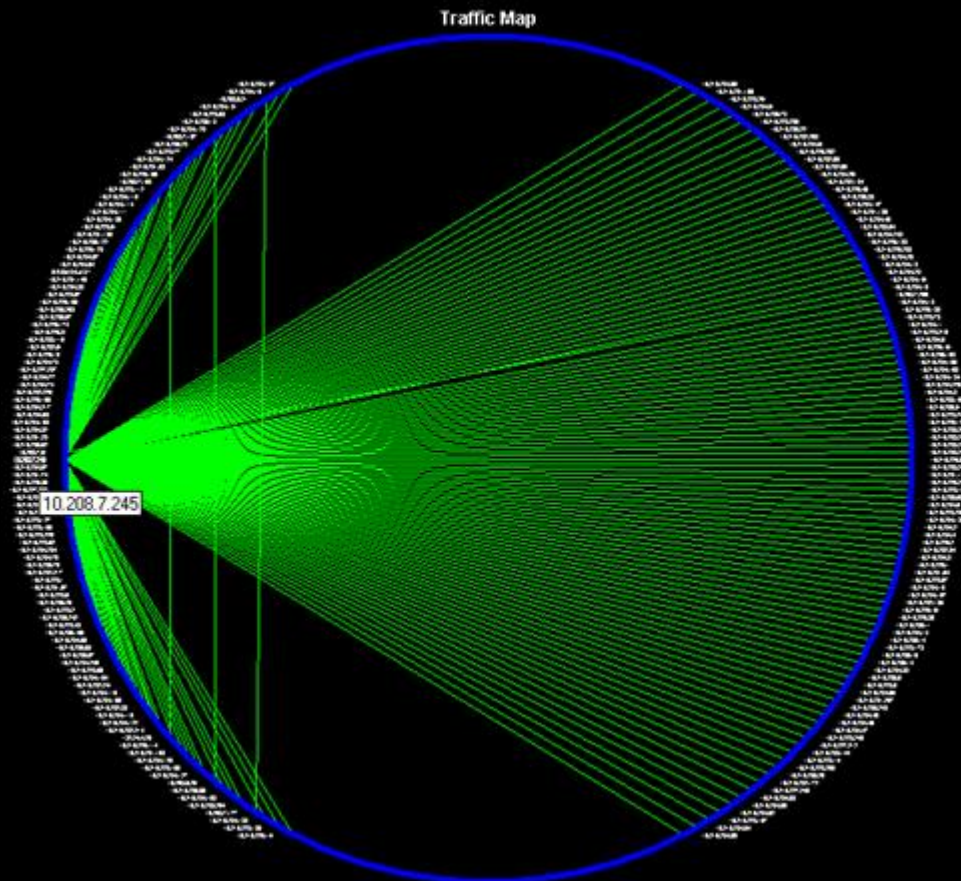
The **BIGGEST** problem in
the world could have been
SOLVED when it was **SMALL**

Malware Name	Date Vulnerability Announced	Date Virus Released	Days Pre-warning
Nimba	Mar 29, 2001	Sep 18, 2001	173
Bugbear	Mar 29, 2001	Sep 30, 2001	185
Slammer	Jul 24, 2002	Jan 25, 2003	185
Nachi	Jul 16, 2003	Aug 18, 2003	33

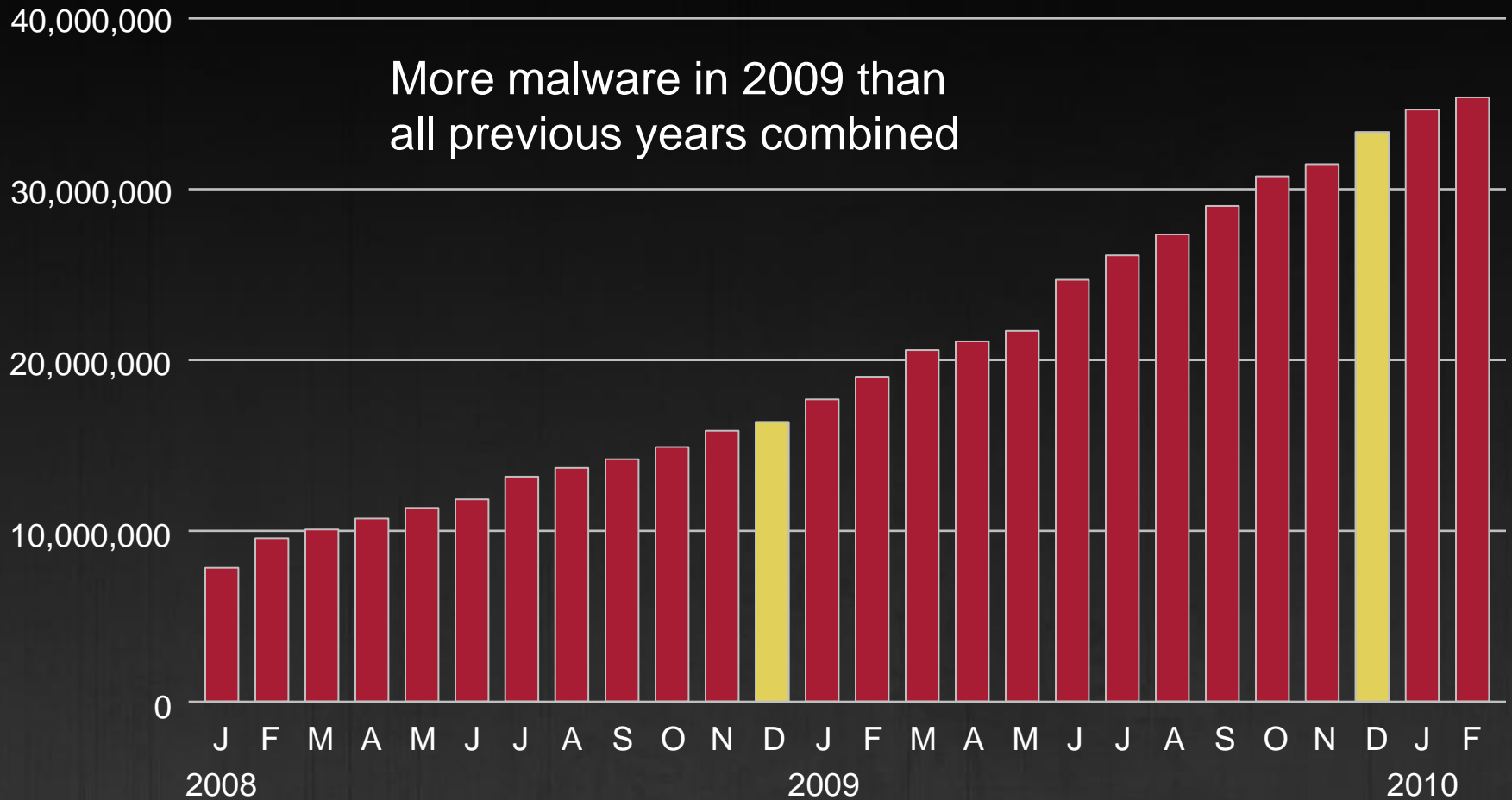
However...



THREATS move at the SPEED OF LIGHT



EXPONENTIAL malware GROWTH



Some startling **STATISTICS**

McAfee reviews about

100,000

Potential malware samples per day

Some startling **STATISTICS**

McAfee identifies over

47,000

New unique pieces of malware per day

Some startling **STATISTICS**

McAfee identifies about

200,000

new zombies per day

Some startling **STATISTICS**

McAfee identifies about

2,000,000

new malicious Web sites per month

Threats play on **SEASONAL** and **SENSATIONAL** topics

Do your research and work only with those services that have a well-established reputation.



2010 FIFA WORLD CUP SOUTH AFRICA
KE. NAKO. Celebrate Africa's Humanity™

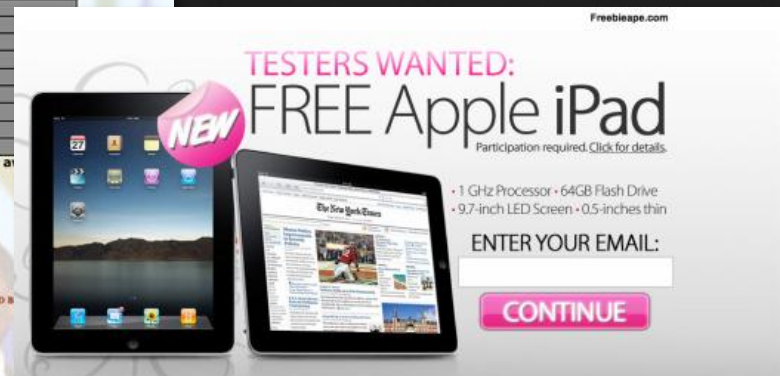
CONGRATULATIONS WINNING NOTIFICATION!!!
SOUTH AFRICAN 2010 FIFA WORLD CUP LOTTERY AWARD

The Global Mega-Million Lottery (GMML) Promotion team is proud to inform you that you have won US\$950,000.00 (Nine Hundred and Fifty Thousand United State Dollars) why you have won? Your E-mail address is one of 7 lucky Addresses who have won in the weekly Promotion.
See below how to claim your prize.
Details on the Winnings
Your Winning Reference Number is: GMML/240142:
Batch Number18/006/1094/LIPDA/ZA
WINNING NUMBERS: 80, 35, 11, 72, 90, 41 (01)
Send the following information below:

FULL NAME:	
NATIONALITY:	
COUNTRY OF RESIDENT:	
CITY:	
AGE:	
SEX:	
MARITAL STATUS	
OCCUPATION:	
COMPANY:	
MOBILE:	
WINNING EMAIL:	
FULL ADDRESS:	

Note: This program is being sponsored by the FIFA SUPPORT TEAM to create a winning 2010 FIFA world Cup, which is to be host by South Africa.
TO FILE FOR YOUR CLAIM...
Contact The Processing Manager:
Mr. Paul Morgan
Tell: [REDACTED]
FAX: [REDACTED]
Email: [REDACTED]

YOU ARE TO CHOOSE YOUR PAYMENT OPTION AT WHICH YOU WANT YOUR FUND PAID TO YOU, LISTED BELOW ARE THE METHODS AND OPTION OF PAYMENT.
(1) TRAVELLING DOWN HERE TO SOUTH AFRICA FOR COLLECTION OF YOUR PRIZE.
(2) ELECTRONIC WIRE TRANSFER
(3) CASHIER CHEQUE PAYMENT
(4) INTERNATIONAL DEBIT CARD



Freebieape.com

TESTERS WANTED:
FREE Apple iPad
Participation required. [Click for details](#)

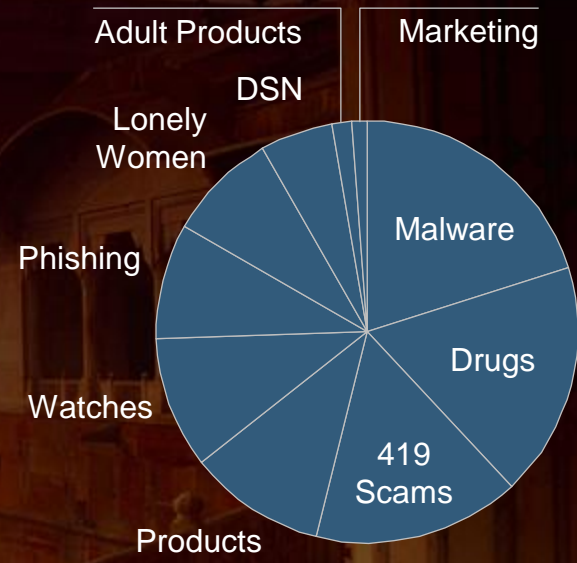
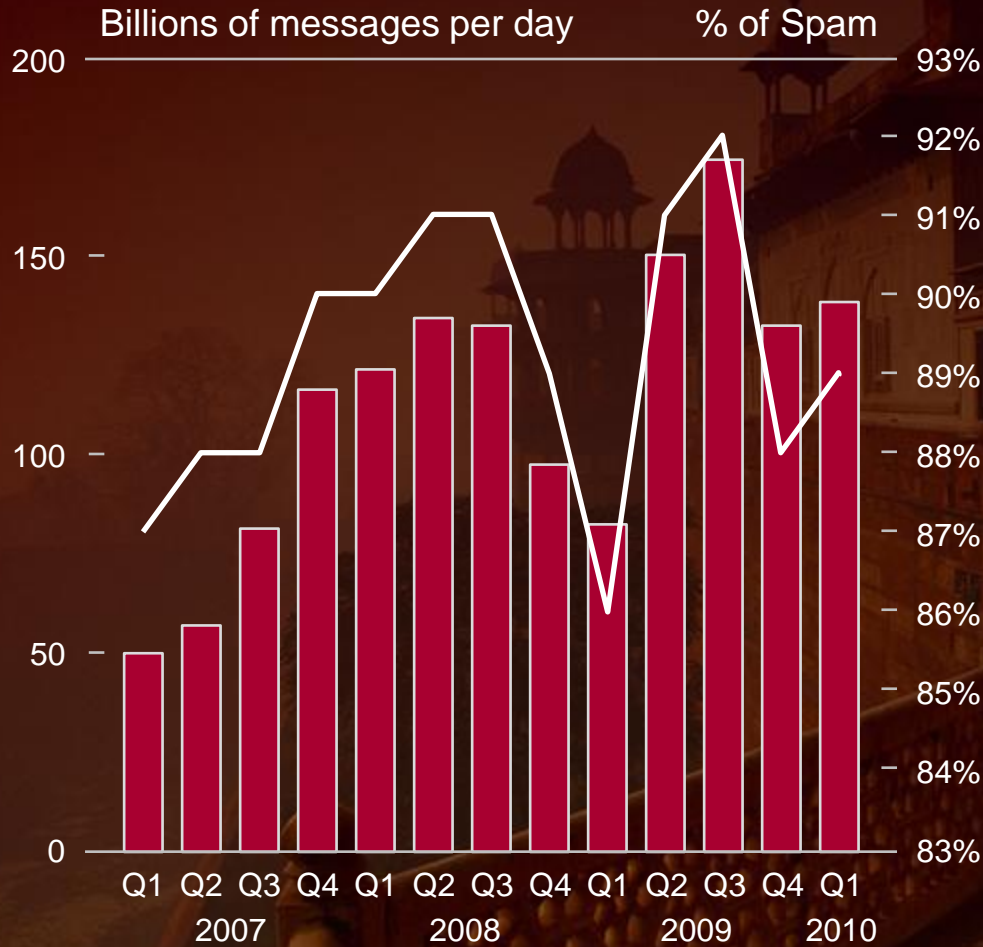
- 1 GHz Processor • 64GB Flash Drive
- 9.7-inch LED Screen • 0.5-inches thin

ENTER YOUR EMAIL:

CONTINUE



Spam and **MALWARE** still **STRONG** in India



From drugs to diplomas, each region's spammers take a different approach

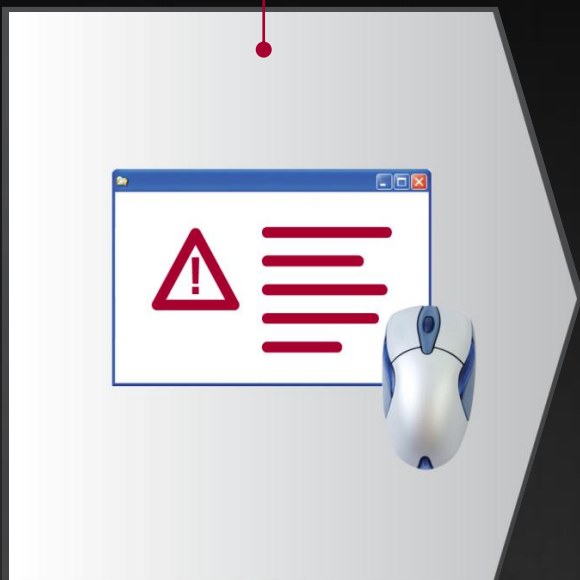
419 scams = A con based on a tragic story or the promise of a reward

DSN = Delivery Service Notice

The Threat Landscape

Threats are growing more sophisticated, evidenced by Operation Aurora

Highly targeted to individuals within IP-rich organizations



EXE disguised as JPG, encrypted 3x with different keys, unpacked a dozen different files



Custom protocol behaved like SSL, port 443, evaded detection, and gained access to highly valuable corporate IP



1

Attack Initiated

User with IE vulnerability visits website infected with Operation Aurora

2

Attack In Progress

Website exploits vulnerability; malware (disguised as JPG) downloaded to user system

3

Attack Setup Complete

Malware installed on user system; malware opens back door (using custom protocol acting like SSL) that gives access to sensitive data

Situational
AWARENESS
is **CRITICAL**

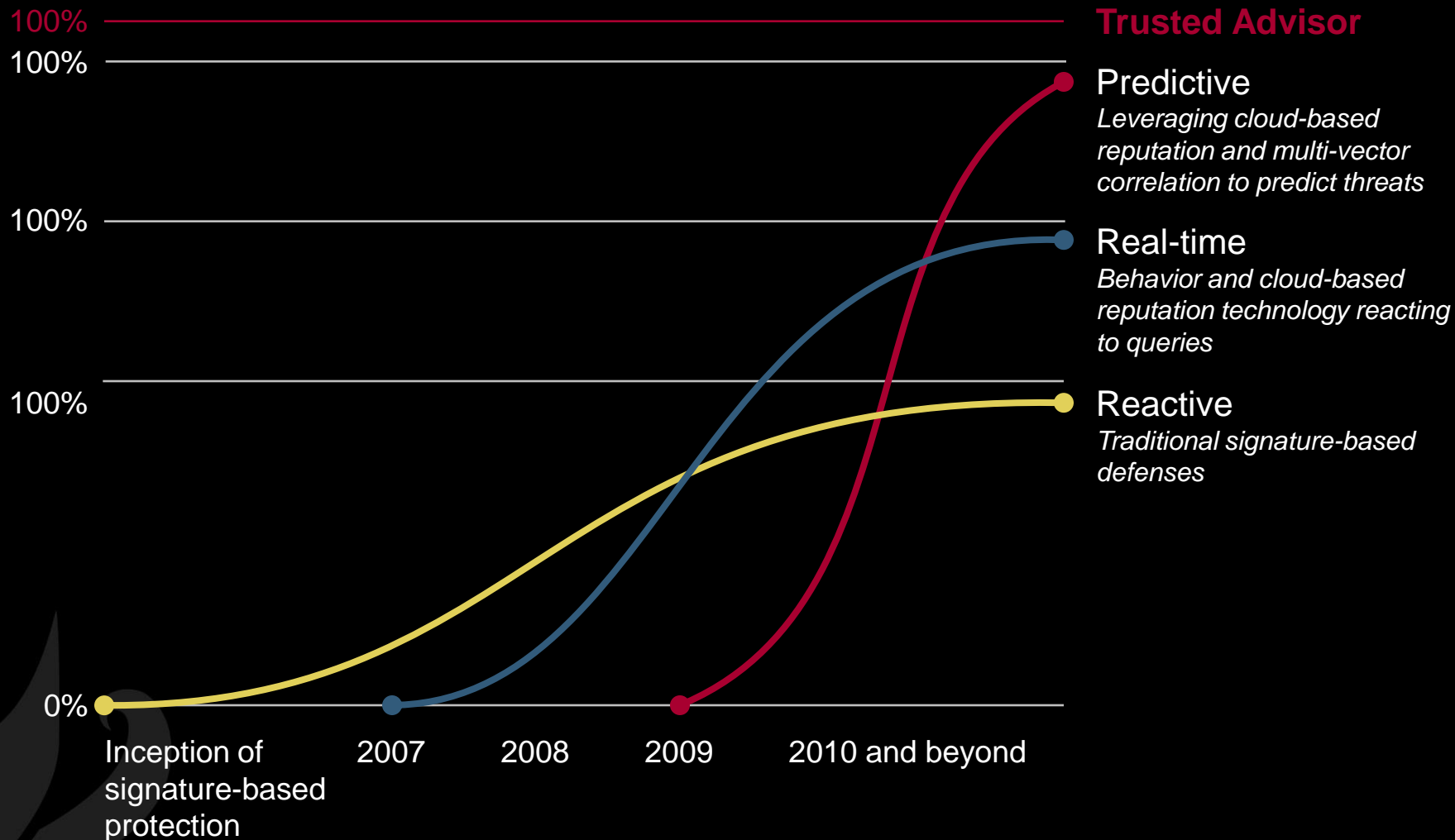


Situational **AWARENESS** in the
security **WORLD** is real too



Facebook Password
Reset Malware

The evolution of **THREAT DETECTION**



YES <OR> **NO**

REACTIVE



How do we solve this problem?

THE CLOUD

What if we could
HARNESS the **POWER**
of the community?





SECURITY TELEMETRY DATA



SECURITY TELEMETRY DATA



The **FUTURE** is...

THE FUTURE IS...



REPUTATION

SCORE

YES

NO

PROACTIVE

The future is
REPUTATION AWARE



THE FUTURE IS...



An aerial photograph of a railway station. The image shows a complex network of tracks, with several high-speed trains (TGVs) visible. The trains are white with blue and red accents. The station has a modern design with a long, low platform. The tracks are made of steel rails on a gravel bed. The overall scene is captured from a high angle, looking down on the tracks and trains. The text "THE FUTURE IS" is overlaid in the center of the image in a bold, red, sans-serif font.

THE FUTURE IS

An aerial photograph of a railway yard with several tracks and trains. The tracks are dark and run parallel to each other, with some crossing over others. There are several trains visible, including a blue and white train in the center and a white train on the right. The background shows some industrial buildings and structures.

ENGINE vs. CONTENT

ENGINES are ubiquitous

Content is KING

THE FUTURE IS...

HERE

Spans the Internet including **millions** of sensors

Uses a combination of protection techniques, where **reputation** is a must

Across **all key** threat vectors
file | web | email | network

Global research team **dedicated** solely to GTI

Real-time, “in the cloud” threat **collection** and intelligence **distribution** model

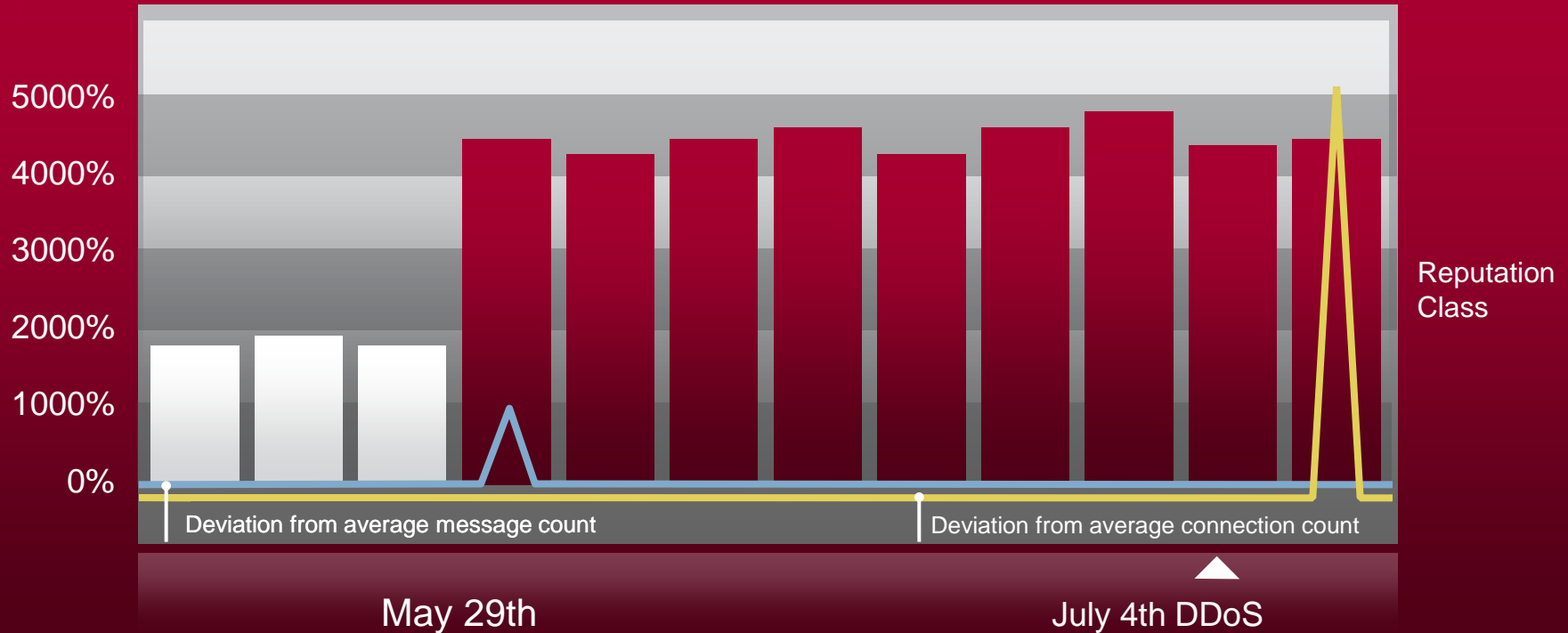
Delivered via a **complete** **suite** of security products



McAfee Global Threat Intelligence in Action



Protecting Against Botnet Attack on U.S. and South Korean Governments



- July 4th 2009: 200,000 zombie Korean botnet launches DDoS against U.S. and South Korean government sites

- McAfee GTI used cross-threat vector correlation to predict the threat and adjusted the reputation of 80% of the IP addresses used to carry out the attack



Where the **RUBBER MEETS** the road

OPTIMIZING your security

Why McAfee is Best Positioned to **DELIVER**

360° Correlation Across All Threat Vectors Allows McAfee to Connect the Dots



Malware

- IP addresses distributing
- URLs hosting malware
- Mail/spam including it
- Botnet affiliation
- IPS attacks caused

Domain/URL

- Mail/spam sending activity
- Web access/referer activity
- Malware hosting activity
- Hosted files
- Popups
- Affiliations
- DNS hosting activity



- Botnet/DDoS activity
- Mail/spam sending activity
- Web access activity
- Malware hosting activity
- Network probing activity
- Presence of malware
- DNS hosting activity
- Intrusion attacks launched

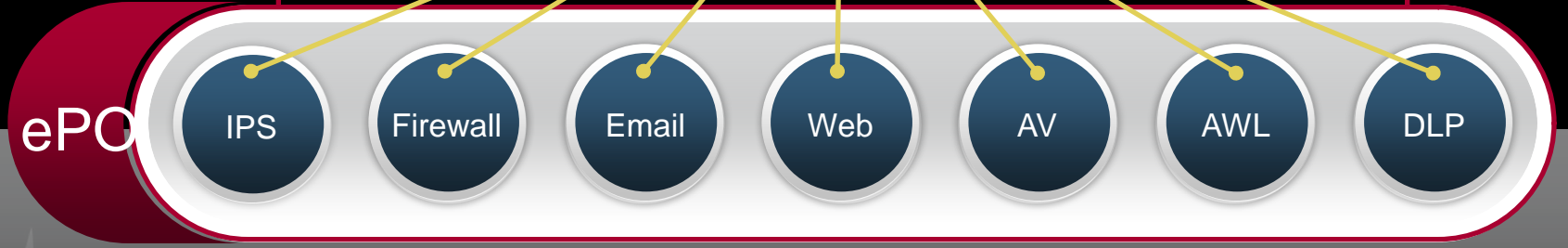
- IP addresses of attackers
- Vulnerability utilized
- Botnet affiliation
- Malware responsible

IP address

IPS attacks/vulnerabilities

Why McAfee is Best Positioned to **DELIVER**

Our Intelligence is Delivered Via a Complete Suite of Products



Endpoint & Data Security



SINGLE management platform for **LOWEST** operating **COSTS**

WHITELISTING, blacklisting, and behavioral **PROTECTION**

COMPREHENSIVE DLP to mitigate **RISK**

Network, Web, and Email Security



FASTEST Network IPS platform

NEXT GENERATION Firewall with true **APPLICATION** awareness

SAFE and productive access to the **INTERNET** and **EMAIL**

Managing Risk & Compliance



COMPREHENSIVE COVERAGE of vulnerabilities

REAL-TIME change monitoring and **PREVENTION** for **PCI Compliance**

Focus on **HIGHEST RISKS** to reduce **COSTS**



GET your
SECURITY program
OFF the **GROUND**



India
**EXECUTIVE
SUMMIT**
A FOCUS SERIES EVENT



Panel



What IT did in 2009

1. Lowered Operating Costs
2. Improved productivity
- 3. Improved security/risk management**
4. Improved quality of products
5. Re-engineered business processes

What IT will do in 2010

1. Drive innovative new products
- 2. Improve security and productivity**
3. Improve quality of processes
4. Re-engineer core processes
5. Lower operating costs

Top IT Management priorities

1. Aligning IT and business goals
- 2. Business continuity/risk management**
3. Controlling IT costs
4. Improving internal user satisfaction
5. Measure & communicate IT value

Major Challenges in 2010



- Chair: Michael Sentonas, CTO and VP,
McAfee Asia Pacific
- Panel Members:
 - Sunil Dhaka, CISO, ICICI Bank
 - Satish Das, Global Chief of Security,
Cognizant Technology
 - Suresh Iyer, CISO APAC, Aditya Birla Minacs

