Vital Threat Management for Enterprise / Carrier

In a Digitally Integrated World

Derek Manky
Project Manager, Cyber Security & Threat Research

CMMA: June 17th, 2009

Presentation Overview

Vital Threat Management For:

- Enterprise & APAC
  - Malware Trends
- Cost Effective, Next Generation Security
  - The Threatscape Today
  - Layered Security
- Mobile Threats
- Q&A

Enterprise & APAC

Targeted Attacks

- Documents Favored
  - Various Exploits Used
    - PDF, XLS, DOC
  - Common Malware Dropped

- Social Engineering 2.0
  - Location Based Services
  - Profiling
    - UPS / DHL Attacks

- Salesforce Snow-Ball Effect
    - **January 31, 2007:** 29,800 Customers
    - **September 2007:** Phishing attacks compromise sensitive data
    - **November 2007:** FTC spoofed attacks with compromised data

Enterprise & APAC

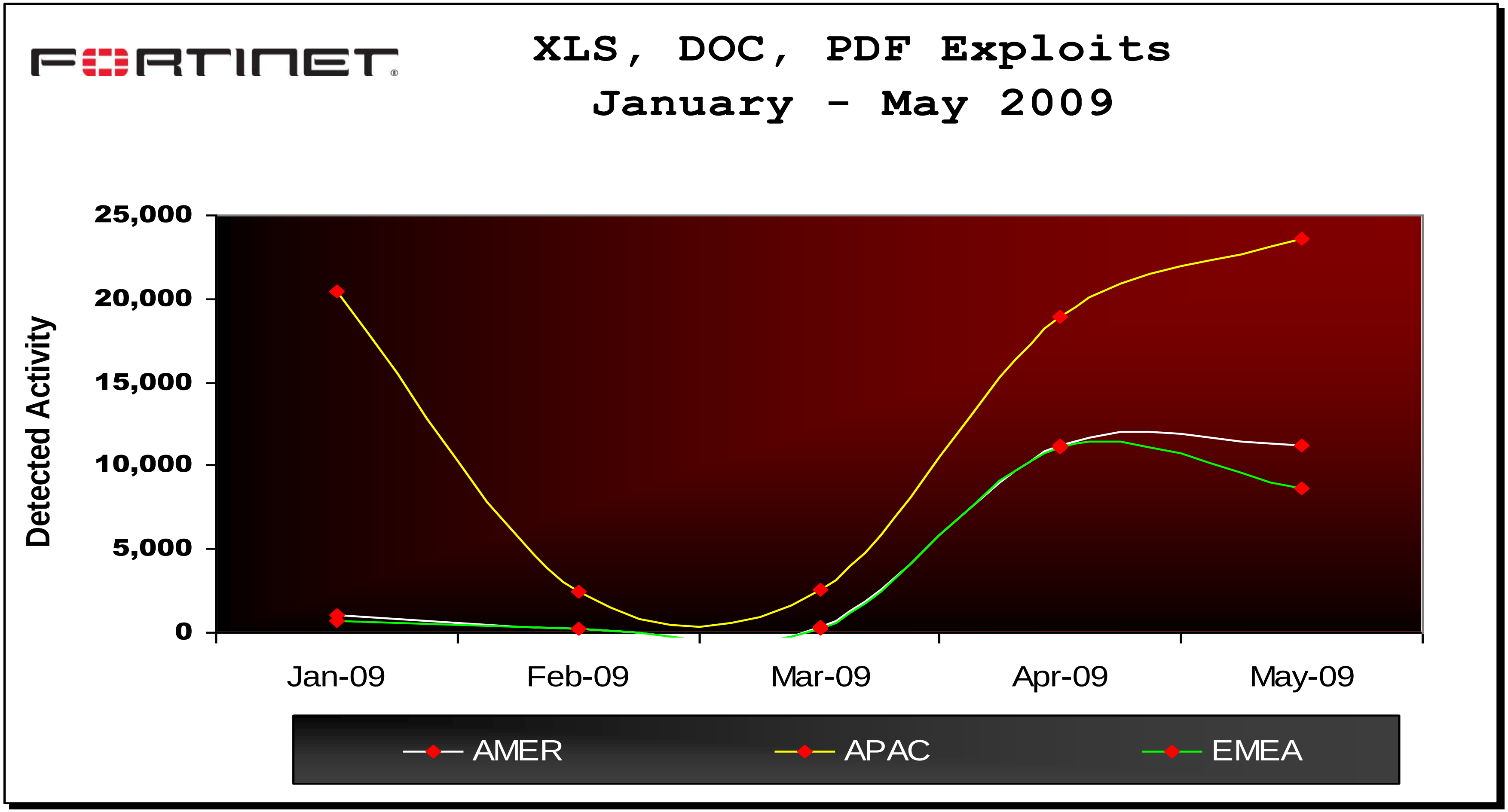
Targeted Attacks

- GhostNet[1]
  - 1,295 unique infections:103 countries
    - Ministry of Foreign Affairs, Embassies
    - Concentration in Asia
  - Spoofed Email (ie: campaigns@freetibet.org)
  - Malicious MS Word document – exploit
  - Drops trojan (Ghost RAT), and innocent document
  - HTTP Communication Used for C&C

GhostNet Source
1: Information Warfare: http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

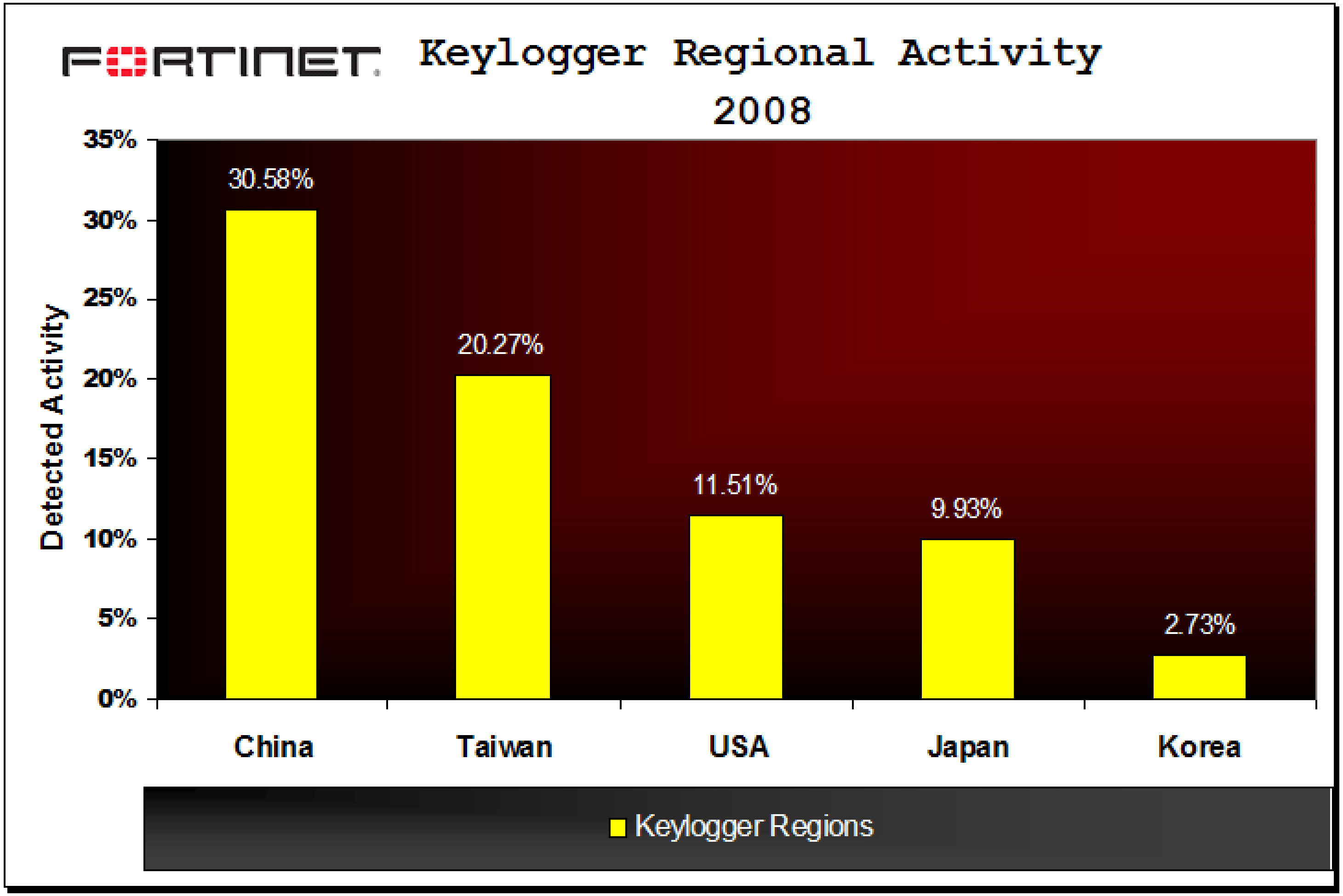
Enterprise & APAC

Targeted Attacks



Enterprise & APAC

Targeted Attacks



Enterprise & APAC

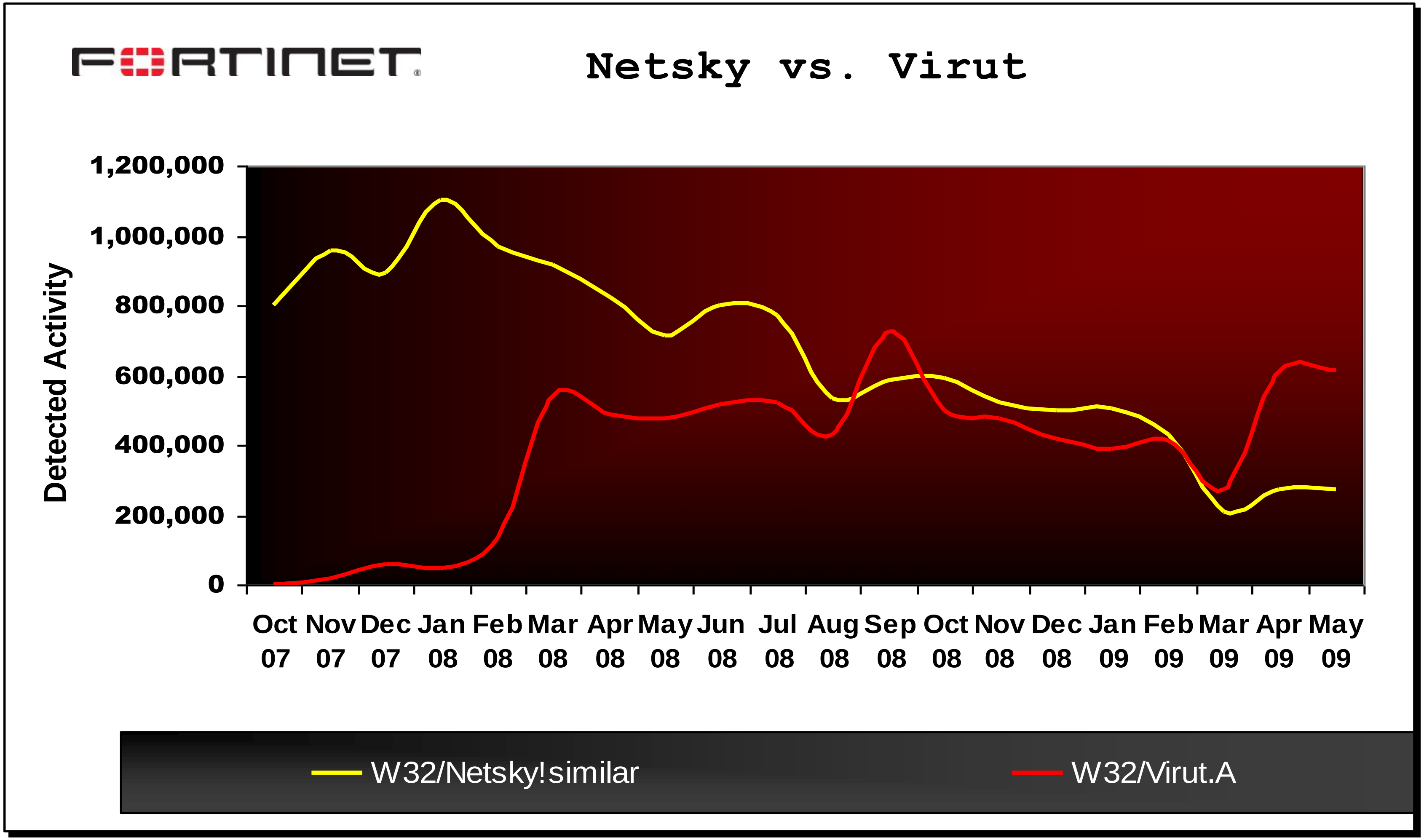
W32/Virut.A

- Dominant in Asia
  - Prevalent for 1+ Years in Korea
- Parasitic File Infector
  - Newly Discovered Hybrids
  - Especially Nasty to Clean

- Hybrid Effect
  - Blended Threats
    - MyDoom, Netsky, Scareware
  - Botnets & Control
  - Polymorphic

Enterprise & APAC

- Volume & Infection Rate Increase Over 1.5 Years



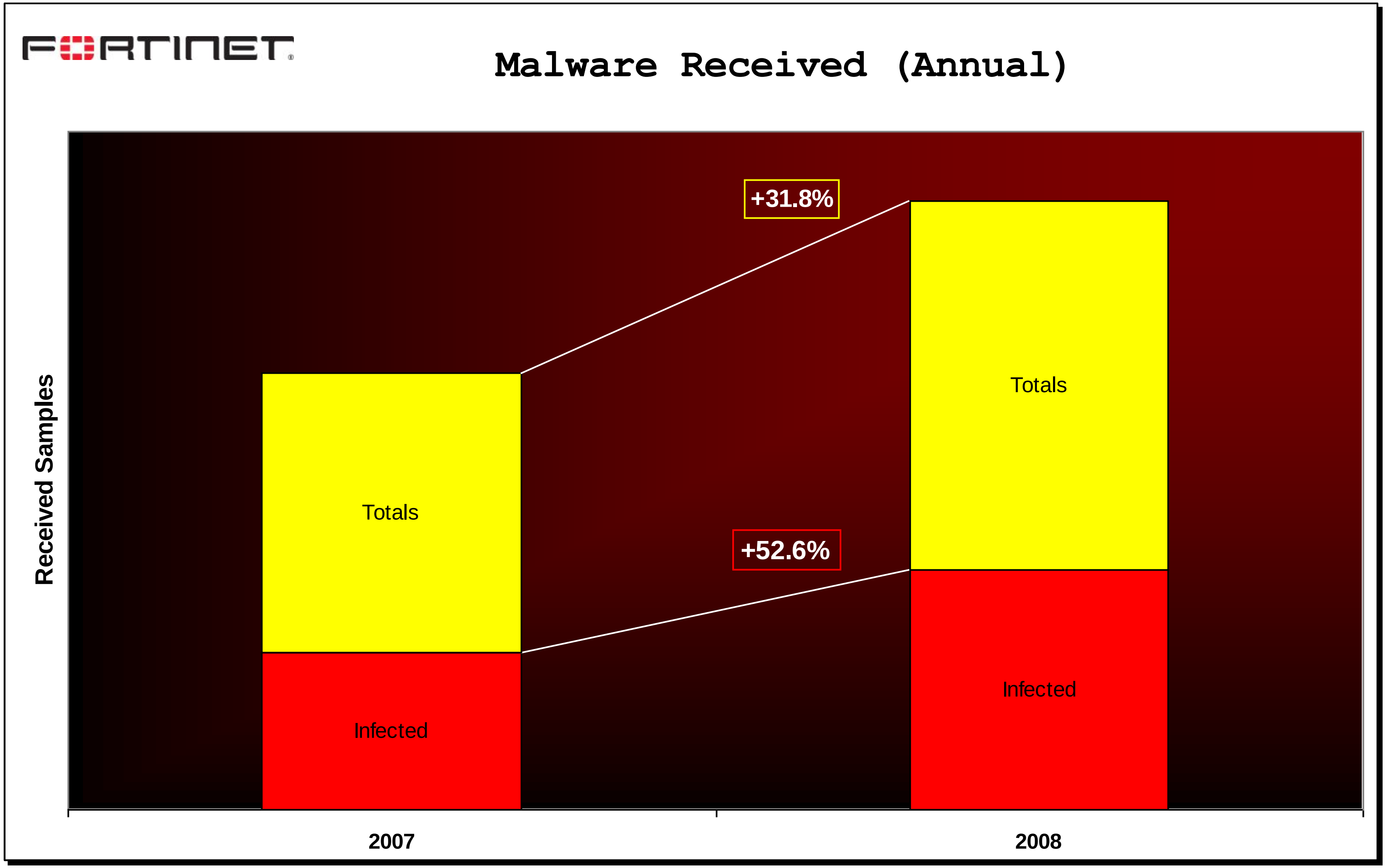
***Source**: Fortinet's FortiGate and Worldwide Intelligence Systems*

Cost Effective
Next Generation Security

Vital Threat Management

Cost Effective, Next Gen Security

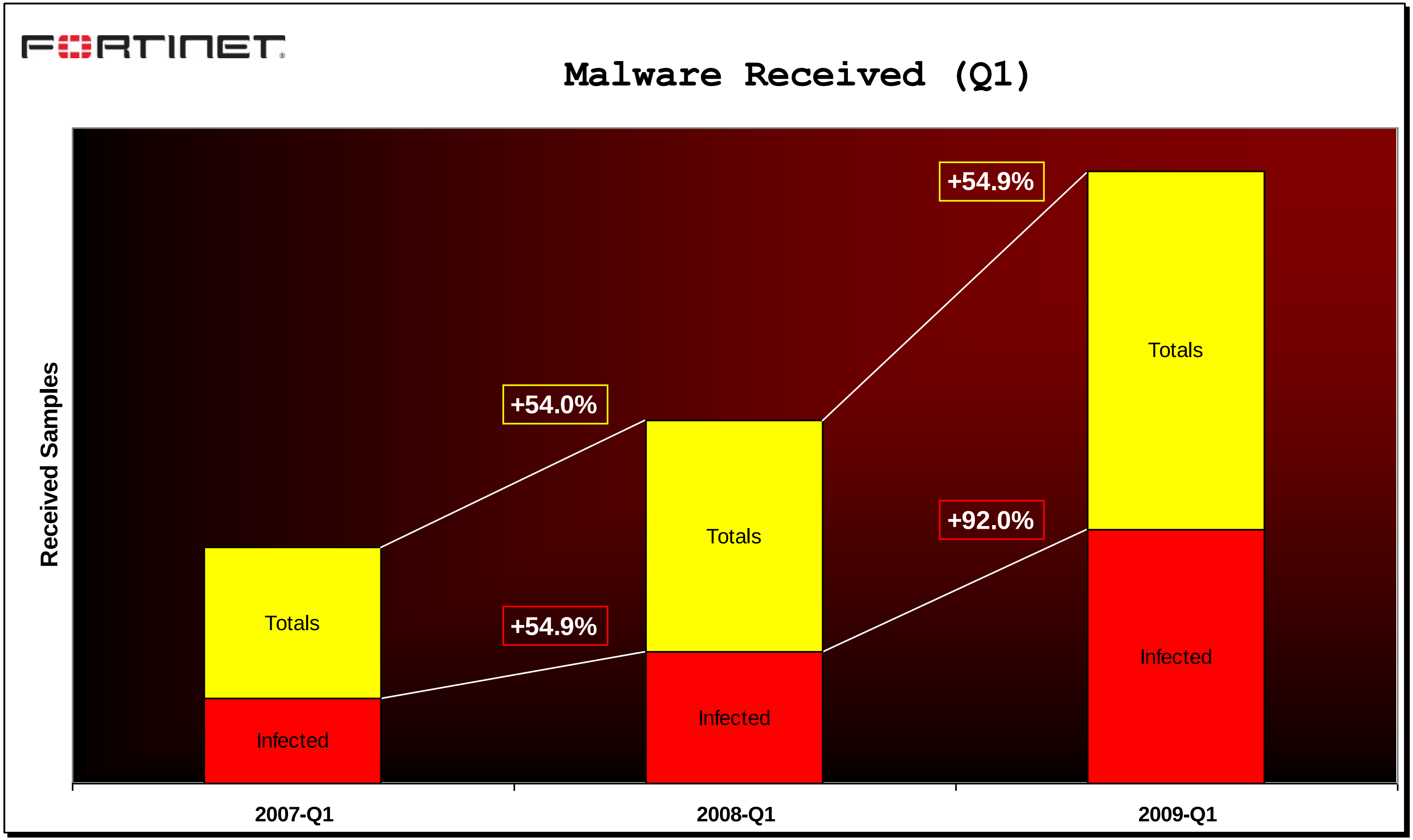
- Volume & Infection Rate Increase Over 2 Years



***Source**: Fortinet's FortiGate and Worldwide Intelligence Systems*

Cost Effective, Next Gen Security

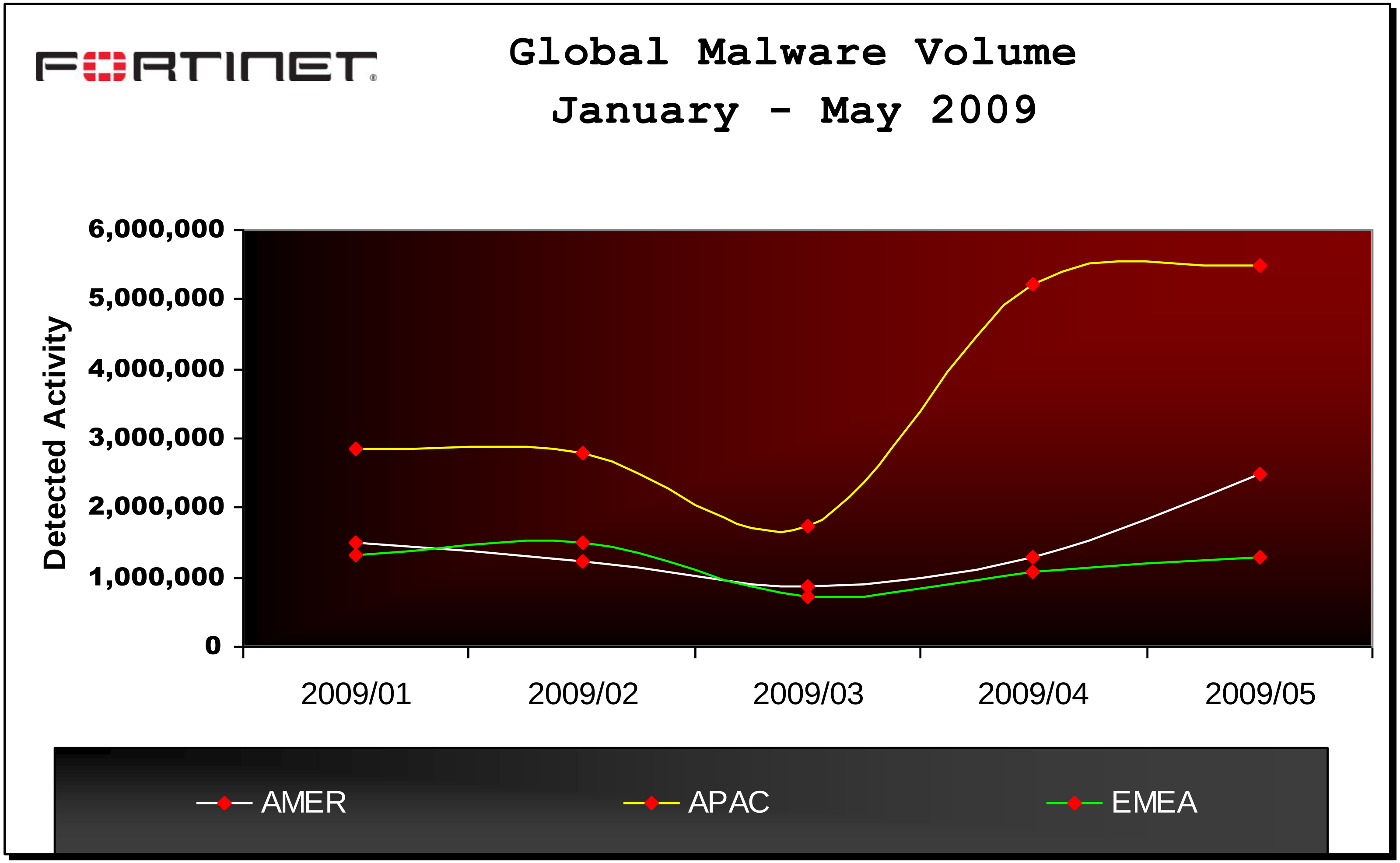
- Volume & Infection Rate Increase Over 3 Quarters



Source: *Fortinet's FortiGate and Worldwide Intelligence Systems*

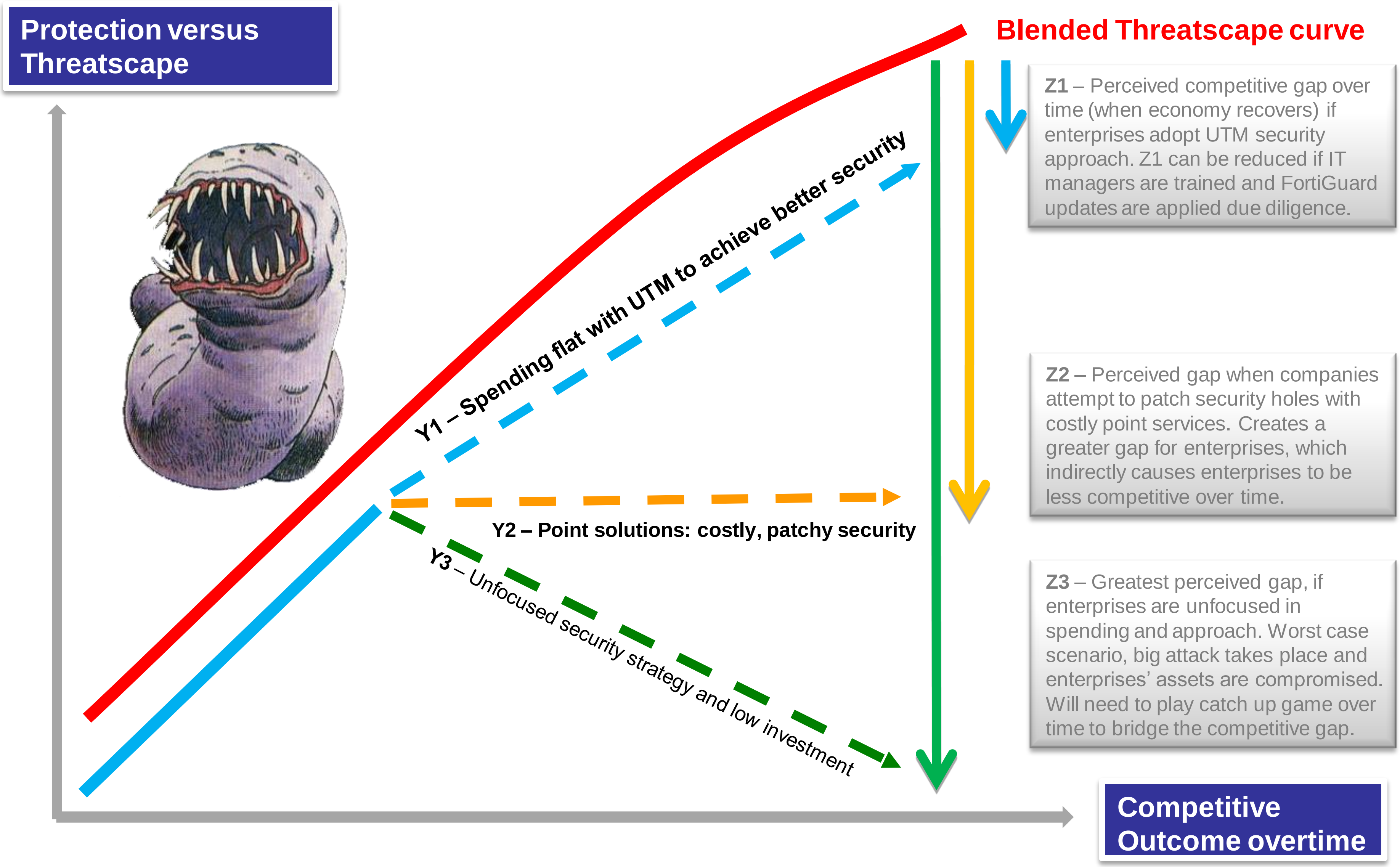
Cost Effective, Next Gen Security

- APAC Leading 2009 Malware Detections



Source: *Fortinet's FortiGate and Worldwide Intelligence Systems*

Ringfence corporate security networks

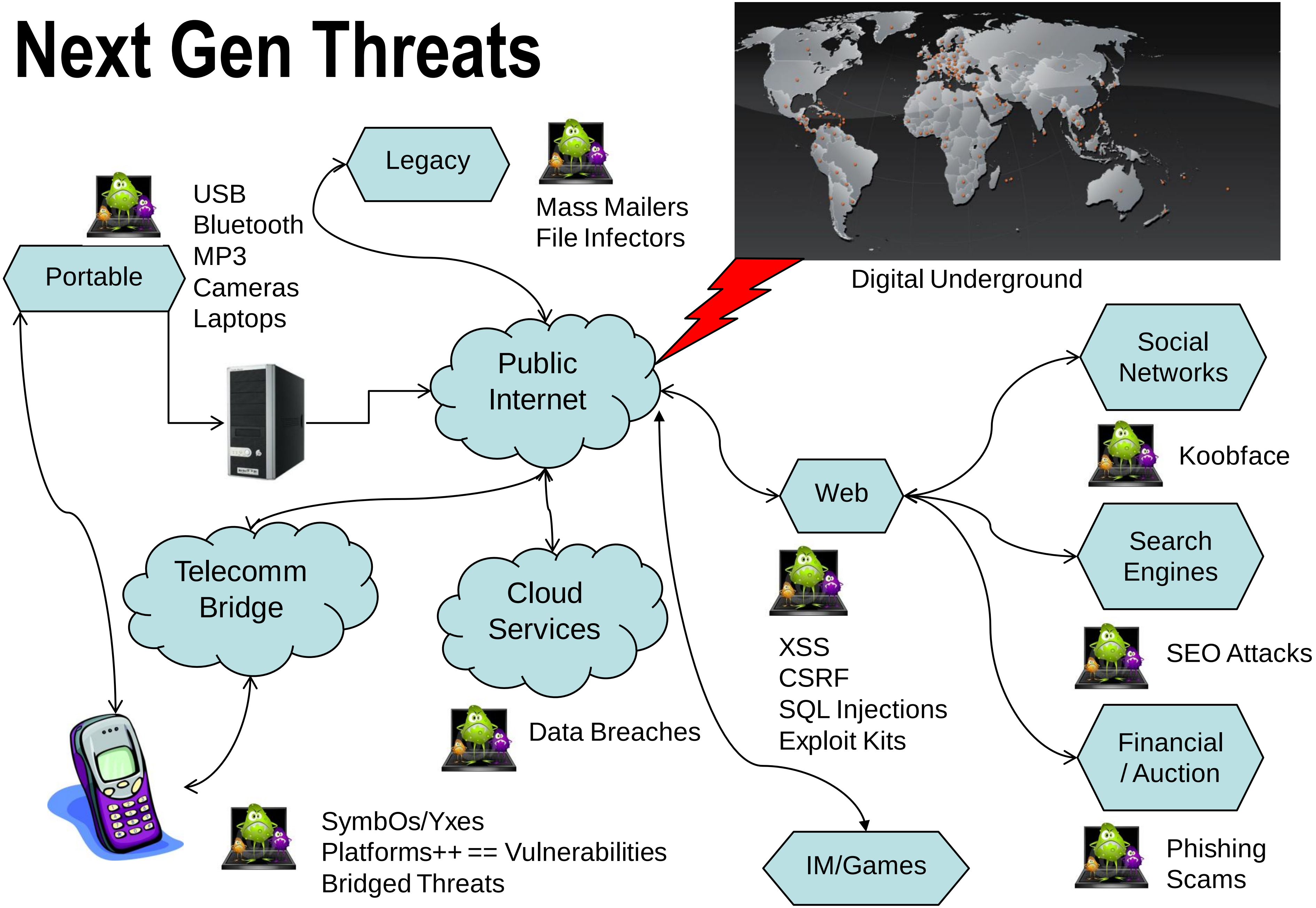

Protection versus Threatscape
Blended Threatscape curve
Y1 – Spending flat with UTM to achieve better security
Y2 – Point solutions: costly, patchy security
Y3 – Unfocused security strategy and low investment
Competitive Outcome overtime

Z1 – Perceived competitive gap over time (when economy recovers) if enterprises adopt UTM security approach. Z1 can be reduced if IT managers are trained and FortiGuard updates are applied due diligence.

Z2 – Perceived gap when companies attempt to patch security holes with costly point services. Creates a greater gap for enterprises, which indirectly causes enterprises to be less competitive over time.

Z3 – Greatest perceived gap, if enterprises are unfocused in spending and approach. Worst case scenario, big attack takes place and enterprises' assets are compromised. Will need to play catch up game over time to bridge the competitive gap.

Next Gen Threats



Legacy

Mass Mailers
File Infectors

Digital Underground

USB
Bluetooth
MP3
Cameras
Laptops

Portable

Public Internet

Social Networks

Koobface

Web

Search Engines

SEO Attacks

Telecomm Bridge

Cloud Services

XSS
CSRF
SQL Injections
Exploit Kits

Data Breaches

Financial / Auction

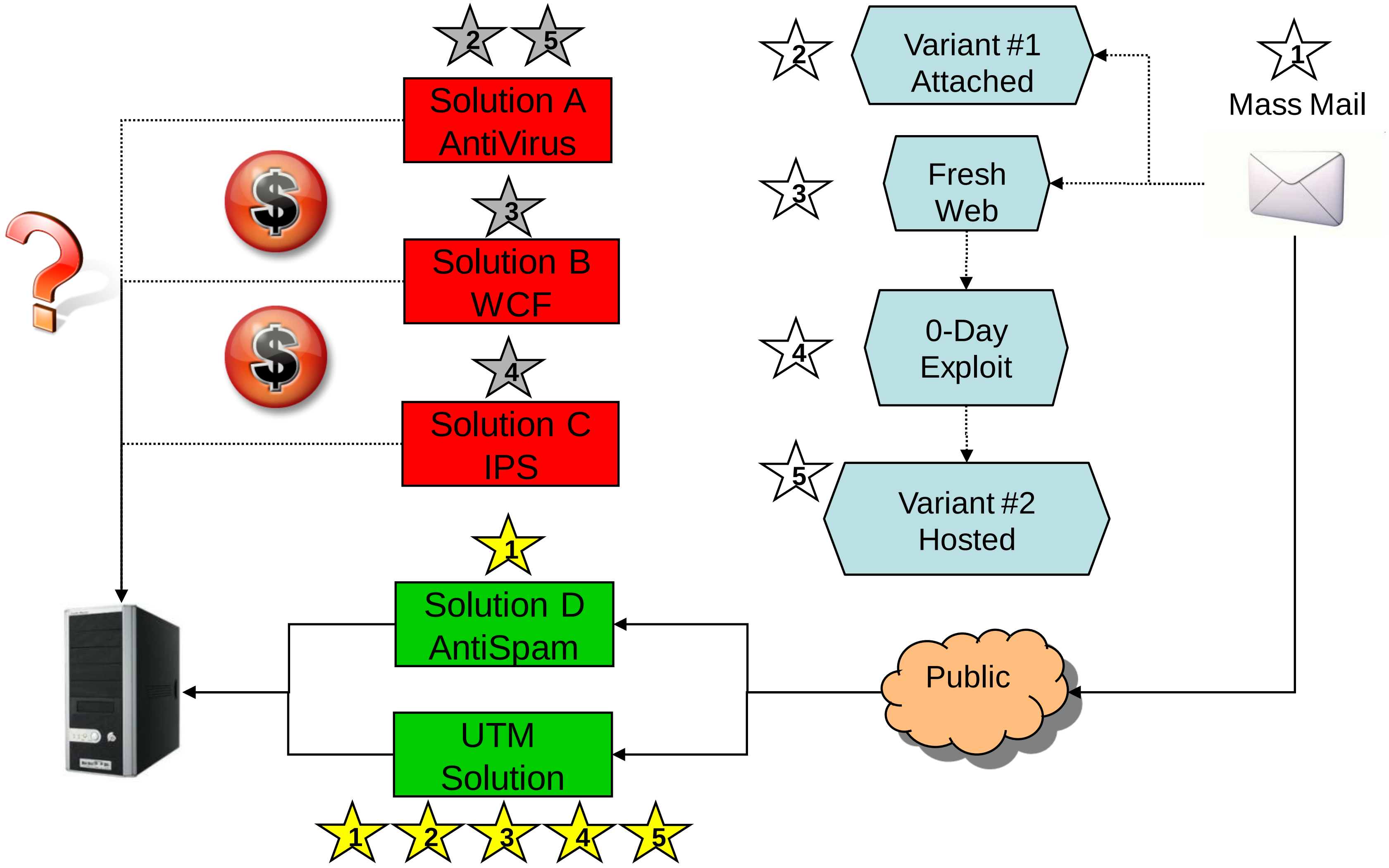
SymbOs/Yxes
Platforms++ == Vulnerabilities
Bridged Threats

IM/Games

Phishing Scams

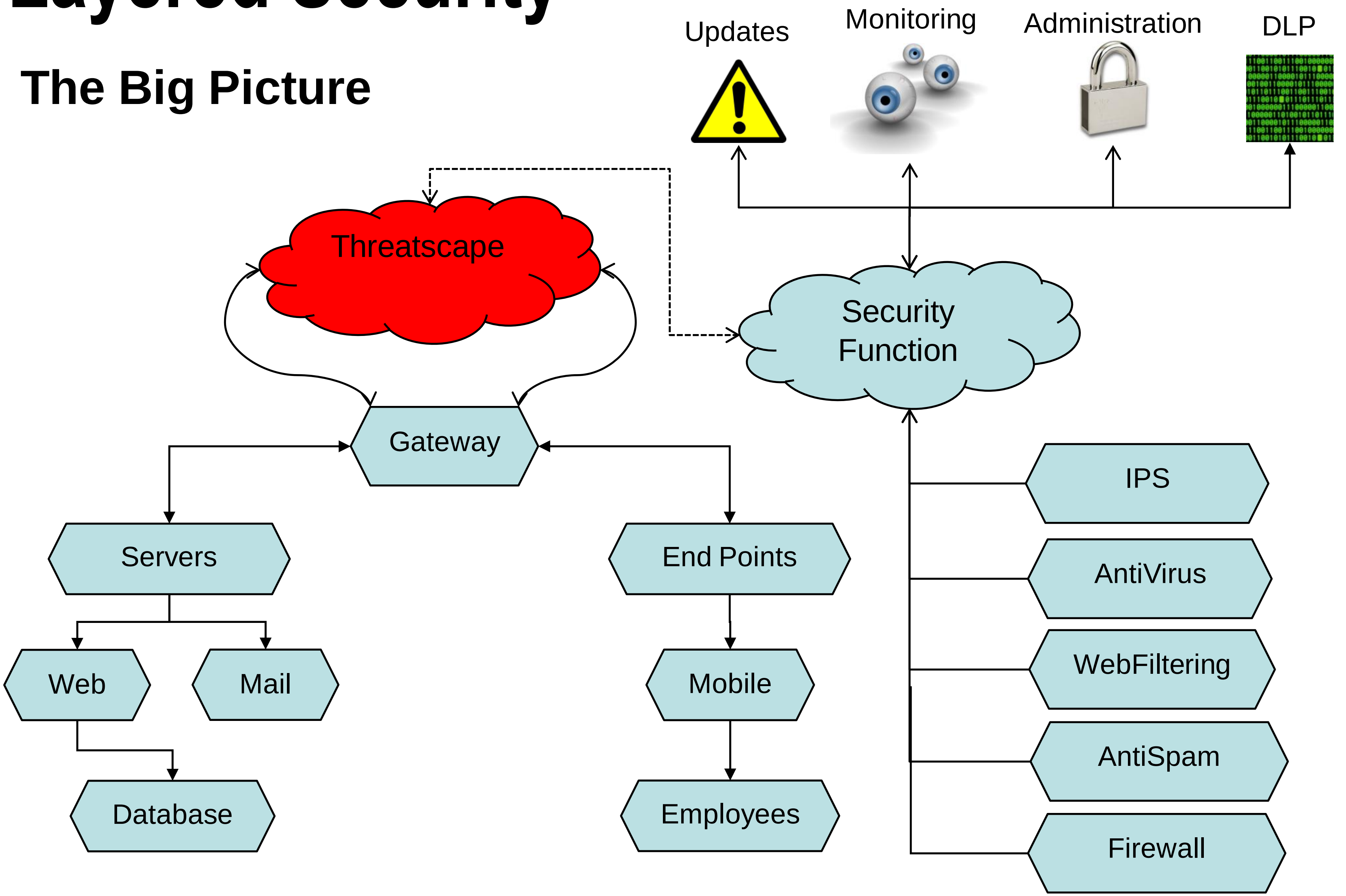
Layered Security

UTM vs. End Point Approach



Layered Security

The Big Picture



Layered Security

Consolidated Approach (UTM)

- Consolidates Management and Deployment
  - Operating Expenses Smoothed
  - Licenses--
- Smaller Footprint
  - Capital Expenditures Reduced
- Scalable to Address:
  - Threat Growth
  - Growing Operations
- Manageable
  - Monitored View of all Threat Vectors
  - Increased Incident Response

Layered Security

In Summary

- Modern Threats Require Layered Solution
  - Too Complex of a Challenge
- Defense in Depth
  - UTM
    - Cost Effective; Security != $$
    - Provides Enhanced Security
    - Both Client & Server Side
  - Policies & Education
- Scalable Solution Required for Threatscape
- Security is Essential
  - Huge Losses Possible
  - Breaches Damage Reputation

Mobile Threats

Vital Threat Management

Mobile Threats on the Rise

Past and Present

2004:

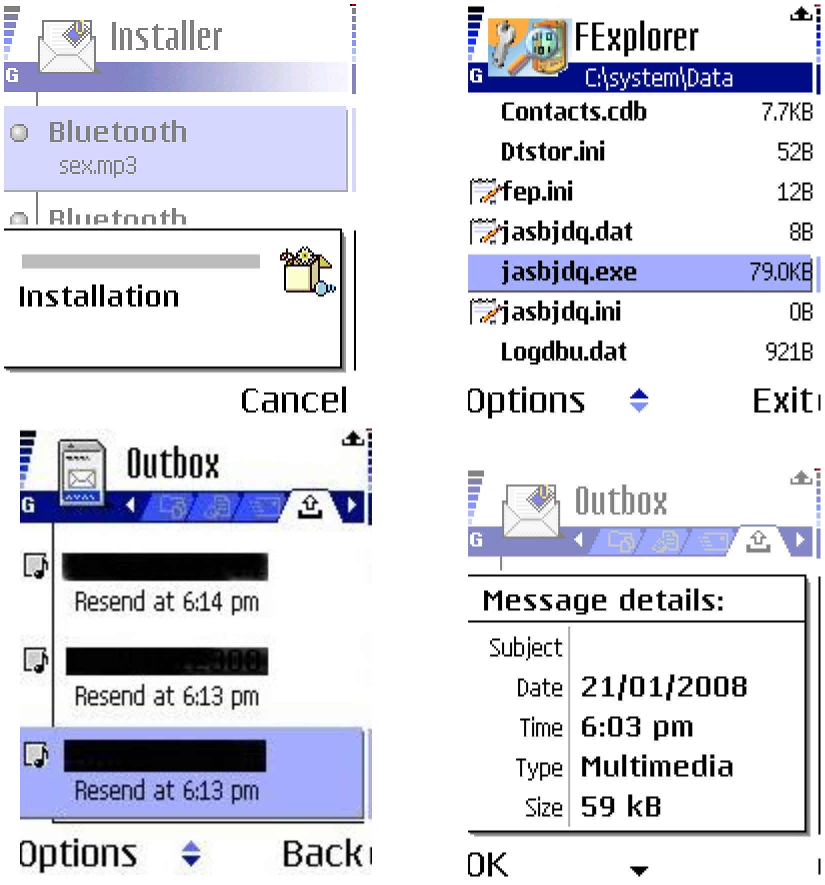
- **SymbOS/Cabir (PoC)**
  - ✓ **Bluetooth**
- **SymbOS/Skulls (DoS)**

2005:

- **SymbOS/CommWarrior**
  - ✓ **Bluetooth, MMS, MMC**

2008/2009:

- **SymbOS/Flocker**
- **SymbOS/BeSeLo**
  - ✓ **File Extension Tricks**
- **SymbOS/CurseSMS (DoS)**
- **SymbOS/Yxes**



FExplorer
C:\system\Data

Contacts.cdb	7.7KB
Dtstor.ini	52B
fep.ini	12B
jasbjdq.dat	8B
jasbjdq.exe	79.0KB
jasbjdq.ini	0B
Logdbu.dat	921B

Outbox

[redacted]
Resend at 6:14 pm

[redacted]
Resend at 6:13 pm

[redacted]
Resend at 6:13 pm

Outbox

Message details:

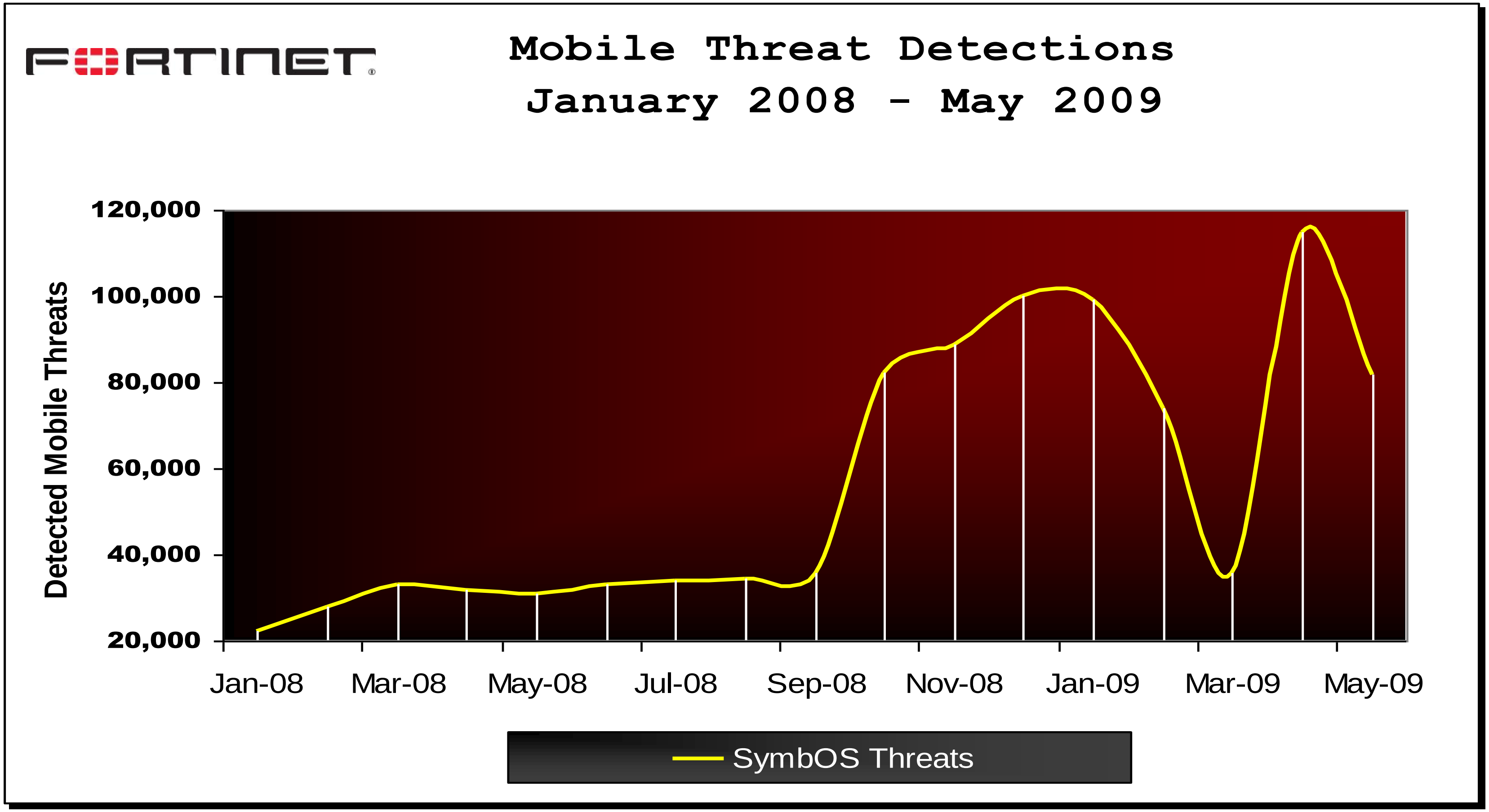
Subject	
Date	21/01/2008
Time	6:03 pm
Type	Multimedia
Size	59 kB

BeSeLo Propagation on S60 Phones

Destruction & Defacement → Monetization

Mobile Threats on the Rise

A Growing Trend

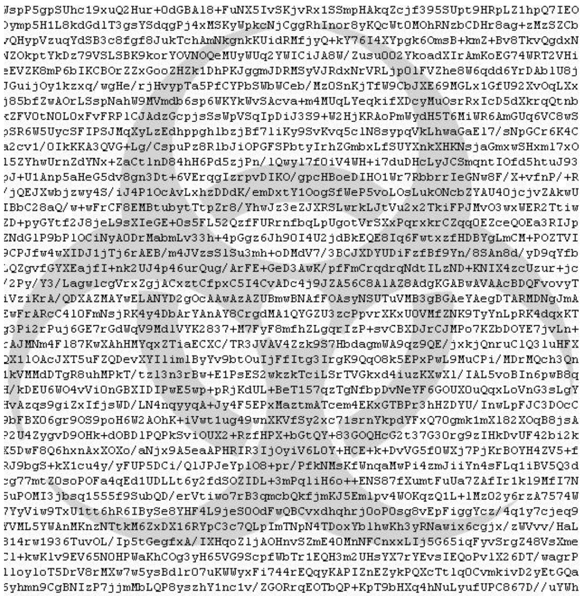


Statistics from Fortinet's network security appliances worldwide

Moving Forward: Securing The Future

Active Threat Ingredients

- Plethora of smart devices
- Increased complexity / functionality
  - ✓ Bridges created
  - ✓ Security holes introduced
- New platforms introduced
- Roaming insider threat
- Adoption of 3G → Roadmap to 4G
  - ✓ Traffic == Cold Hard Cash



```
JspP5gpSUhc19xuQ2Hur+OdGBA18+FuNX5IvSKjvRx1SSmpHAkqZcjf395SUpt9HRpLZ1hpQ7IEO
Dymp5H1L8kdGdlT3gsYSdqgPj4xMSKyWpkcNjCggRhInor8yKQcWtOMOhRNzbCDHr8ag+zMzSZCb
vQHypVzuqYdSB3c8fgf8JukTchAmNkgnkKUidRMfjyQ+kY76I4XYpgk6OmsB+kmZ+Bv8TkvQgdxN
NZOkptYkDz79VSLSBK9korYOVNOQeMUyWUq2YWICiJA8W/ZusuOO2YkoadXIrAmKoEG74WRT2VHi
eEVZK8mP6bIKCBOrZZxGooZHZk1DhPKJggmJDRMSyVJRdxNrVRLjpOlFVZhe8W6qdd6YrDAblU8j
JGuijOy1kzxq/wgHe/rjHvypTa5PfCYPbSWbWCeb/MzOSnKjTfW9CbJXE69MGLx1GfU92XvOqLXx
j85bfZwAOrLSspNahW9MVmdb6sp6WKYkWvSAcva+m4MUqLYeqkifXDcyMuOsrRxIcD5dXkrqQtnb
xZFVOtNOLOxFvFRPlCJAdzGcpjsSsWpVSqIpDiJ3S9+W2HjKRAoPmWydH5T6MiWR6AmGUq6VC8wS
pSR6W5UycSFIPSJMqXyLzEdhppghlbzjBf7liKy9SvKvq5clN8sypqVkLhwaGaEl7/sNpGCr6K4C
a2cv1/OIkKKA3QVG+Lg/CspuPz8RlbJiOPGFSPbtyIrhZGmbxLfSUYXnkXHKNsjaGmxwSHxml7xO
l5ZYhwUrnZdYNx+ZaCtlnD84hH6Pd5zjPn/lQwyl7fOiV4WH+i7duDHcLyJCSmqntIOfd5htuJ93
pJ+U1Anp5aHeG5dv8gn3Dt+6VErqgIzrpvDIKO/gpcHBoeDIHO1Wr7RbbrrIeGNw8F/X+vfnP/+R
/jQEJXwbjzwy4S/iJ4P1OcAvLxhzDDdK/emDxtY1OogSfWeP5voLOsLukONcbZYAU4OjcjvZAkwU
IBbC28aQ/w+wFrCF8EMBtubytTtpZr8/YhwJz3eZJXRSLwrkLJtVu2x2TkiFPJMvO3wxWER2Ttiw
ZD+pyGYtf2J8jeL9sXIeGE+Os5FL52QzfFURrnfbqLpUgotVrSXxPqrxkrCZqqOEZceQOEa3RIJp
ZNdGlP9bPlOCiNyAODrMabmLv33h+4pGgz6Jh9OI4U2jdBkEQE8Iq6FwtxzfHDBYgLmCM+POZTVI
9CPJfw4wXIDJ1jTj6rAEB/m4JVzsSlSu3mh+oDMdV7/3BCJXDYUDiFzfBf9Yn/8SAn8d/yD9qYfb
LQZgvfGYXEajfI+nk2UJ4p46urQug/ArFE+GeD3AwK/pfFmCrqdrqNdtILzND+KNIX4zcUzur+jc
/2Py/Y3/LagwlcgVrxZgjACxztCfpxC5I4CvADc4j9JZA56C8AlAZ8AdgKGABwAVAAcBDQFvovyT
iVziKrA/QDXAZMAYwELANYD2gOcAAwAzAZUBmwBNAfFOAsyNSUTuVMB3gBGAeYAegDTARMDNgJmA
EwFrARcC41OFmNsjRK4y4DbArYAnAY8CrgdMA1QYGZU3zcPpvrXKxUOVMfZNK9TyYnLpRK4dqxKT
g3Pi2rPuj6GE7rGdWqV9MdlVYK2837+M7FyF8mfhZLgqrIzP+svCBXDJrCJMPo7KZbDOYE7jvLn+
cAJMNm4Fl87KwXAhHMYqxZTiaECXC/TR3JVAV4Zzk9S7HbdagmWA9qz9QE/jxkjQnruClQ3luHFX
QX1lOAcJXT5uFZQDevXYIlimlByYv9btOuIjFfItg3IrgK9QqO8k5EPxPwL9MuCPi/MDrMQch3Qn
1kVMMdDTgR8uhMPkT/tzl3n3rBw+E1PsES2wkzkTciLSrTVGkxd4iuzKXwXl/IAL5voBIn6pwB8q
H/kDEU6WO4vViOnGBXIDIPwE5wp+pRjKdUL+BeT157qzTgNfbpDvNeYF6GOUXOuQqxLoVnG3sLgY
HvAzqs9giZxIfjsWD/LN4nqyyqA+Jy4F5EPxMaztmATcem4EKxGTBPr3hHZDYU/InwLpFJC3DOcC
9bFBXO6gr9OS9poH6W2AOhK+iVwt1ug49wnXKVfSy2xc71srnYkpdYFxQ7Ogmk1mXl82XOqB8jsA
P2U4ZygvD9OHk+dOBDlPQPkSviOUX2+RzfHPX+bGtQY+83GOQHcG2t37G3Org9zIHkDvUF42bi2k
X5DwF8Q6hxnAxXOXo/aNjx9A5eaAPHRIR3IjOyiV6LOY+HCE+k+DvVG5fOWXj7PjKrBOYH4ZV5+f
RJ9bgS+kX1cu4y/yFUP5DCi/QlJPJeYplO8+pr/PfkNMsKfWnqaMwPi4zmJiiYn4sFLq1iBV5Q3d
cg77mtZOsoPOFa4qEd1UDLLt6y2fdSOZIDL+3mPqliH6o++ENS87fXumtFuUa7ZAfIr1kl9MfI7N
5uPOMI3jbsq1555f9SubQD/erVtiwo7rB3qmcbQkfjmKJ5Emlpv4WOKqzQ1L+lMzO2y6rzA7574W
7YyViw9TxU1tt6hR6IBySe8YHF4L9jeSOOdFwQBCvxdhqhrjOoPOsg8vEpFiggYcz/4q1y7cjeq9
YVML5YWAnMKnzNTtkM6ZxDX16RYpC3c7QLpImTNpN4TDoxYblhwKh3yRNawix6cgjx/zWVvv/HaL
314rw1936TuvOL/Ip5tGegfxA/IXHqoZljAOHnvSZmE4OMnNFCnxxLIj5G65iqFyvSrgZ48VsXme
Cl+kwKlv9EV65NOHPWaKhCOg3yH65VG9ScpfWbTr1EQH3m2UHsYX7rYEvsIEQoPvlX26DT/wagrP
lloyloT5DrV8rMXw7w5ysBdlrO7uKWWyxFi744rEQqyKAPIZnEZykPQXcTtlqOCvmkivD2yEtGQa
5yhmn9CgBNIzP7jjmMbLQP8yszhY1nc1v/ZGORrqEOTbQP+KpT9bHXq4hNuLyufUPC867D//uYWh
```

On The Horizon

- Increased integration
  - ✓ Smart devices & cloud services
- Digital underground invests
  - ✓ Custom malware / targeted attacks
  - ✓ Zero-days, roaming botnets

Moving Forward: Securing The Future

Protecting Against Attacks

- **Enterprise Security**
  - ✓ **Endpoint Solution (Roaming)**
  - ✓ **Gateway Solution (Bridged)**
  - ✓ **Policies & Education**

- **Carrier Security**
  - ✓ **Gateway Solution (MMS)**
  - ✓ **Monitoring & Alerts**

- **Vendor Security**
  - ✓ **Safe Coding / R&D Practices**
  - ✓ **Responsible Disclosure**

✓ ***FortiCarrier***
✓ ***FortiClient Mobile***
✓ ***FortiGuard Global Security Research Team***

Questions ?

Thank You!