RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

What Are Your Key Definitive Strategies Against Advanced Persistent Threat Today?

A New, Modern Approach - Blue Coat Advanced Threat Protection

SESSION ID: SPO-T11

Brian Shen

Head of Product Marketing, APAC & Japan
Blue Coat Systems

LANDSCAPE
ADVANCED THREATS
COUNTER MEASURES

Today's digital enterprise is driving a new it paradigm…

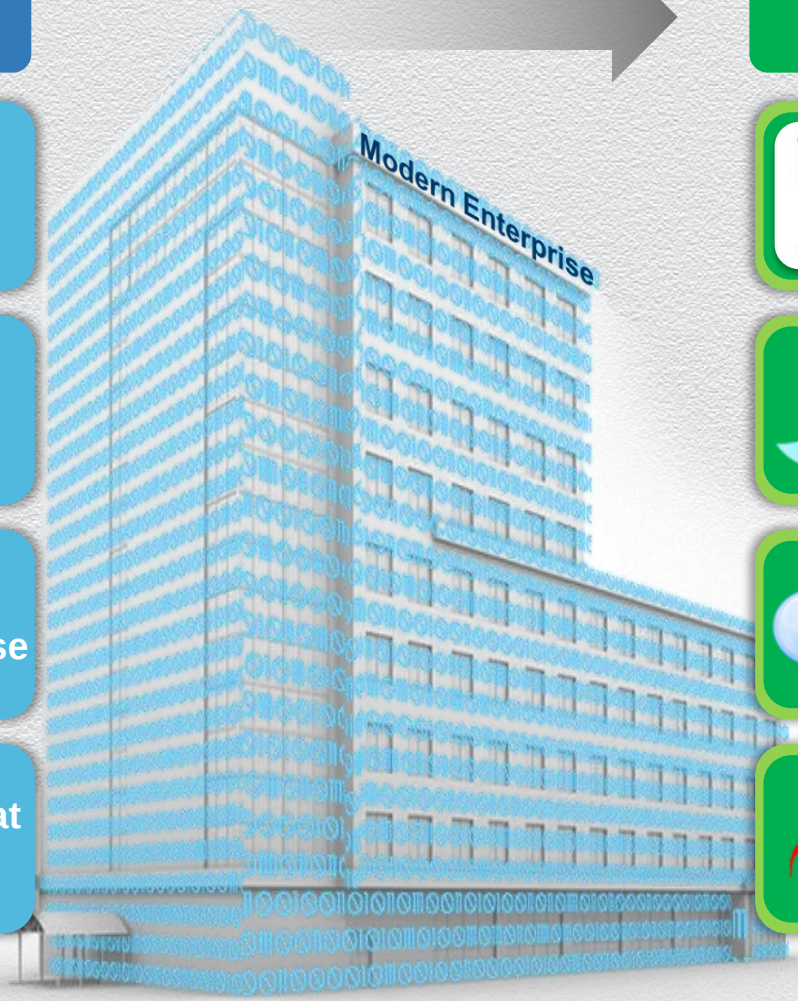
- Cloud / Virtualization
- Big Data Analytics
- Enterprise Social
- SaaS
- Mobility
- Security

BLUE COAT

…and a whole new set of IT challenges

YESTERDAY'S IT

- Few apps with predictable behavior
- Manageable data
- Infrastructure that's on-premise
- Traditional threat environment



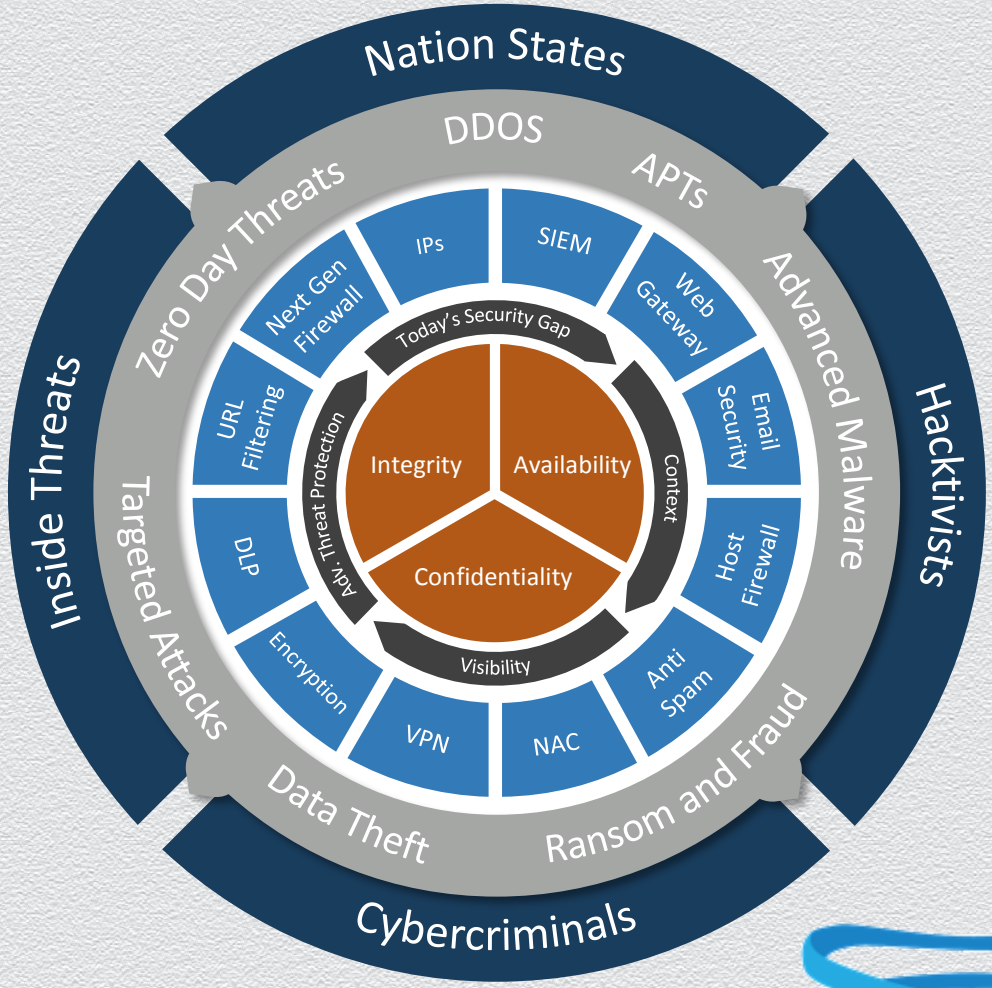
TODAY'S IT

- Millions of unknown and risky Apps
- Big data explosion
- Cloud and hybrid infrastructure
- Advanced threat environment

BLUE COAT

Evolving landscape of modern threats

TODAY'S ADVANCED THREAT LANDSCAPE



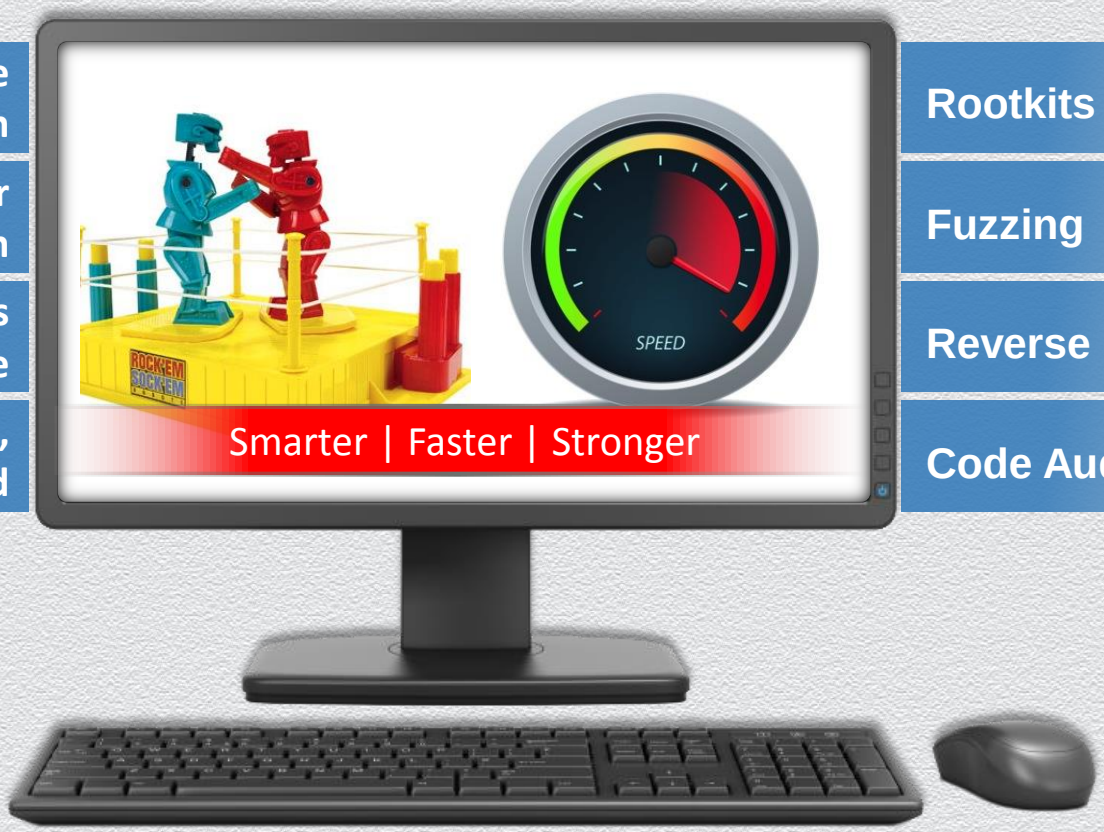
BLUE COAT

#RSAC

RSACONFERENCE2014 ASIA PACIFIC & JAPAN

Improved sophisticated threats

- Virtual machine Detection
- Line-by-line debugger detection
- Re-writes host file
- Multi-packed, one time, encrypted



- Rootkits
- Fuzzing
- Reverse Engineering
- Code Auditing

BLUE COAT

#RSAC

RSA CONFERENCE 2014 ASIA PACIFIC & JAPAN

Danielle Walker, Reporter
Follow @daniellewlkr

October 07, 2013

"Gameover" trojan hides activity in encrypted SSL connections to defraud victims

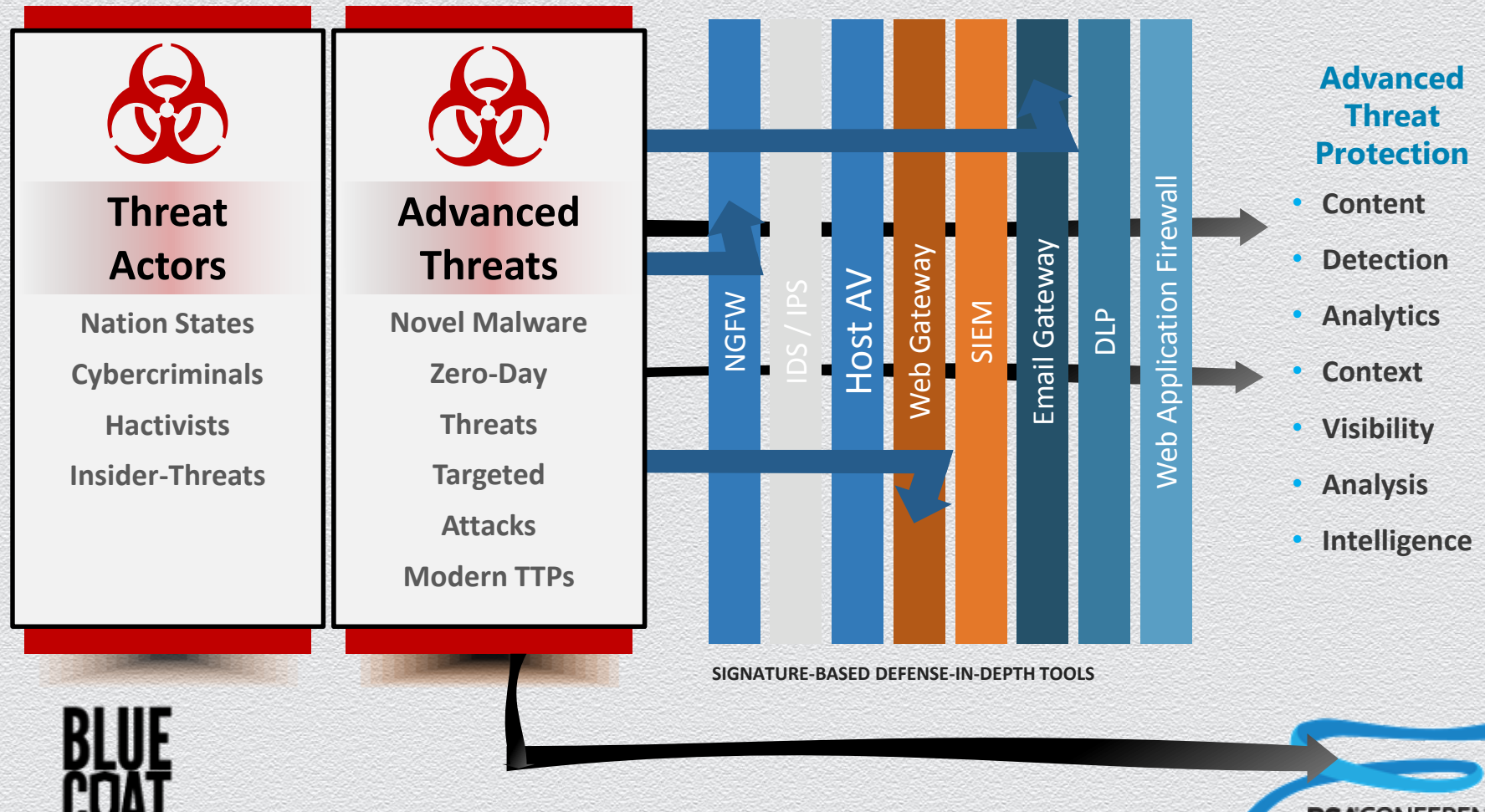
Saboteurs spreading the Gameover banking trojan are hosting the Zeus variant on a number of infected websites and using an encrypted secure sockets layer (SSL) connection to remain undetected.

Researchers at Dell SecureWorks Counter Threat Unit (CTU) detailed attackers' latest schemes to spread the financial malware in a blog post published last Friday.

According to the team, Gameover operators are delivering downloader malware called "Upatre" to victims via spam, then having the downloader retrieve the Gameover payload from infected websites hosting the malware.

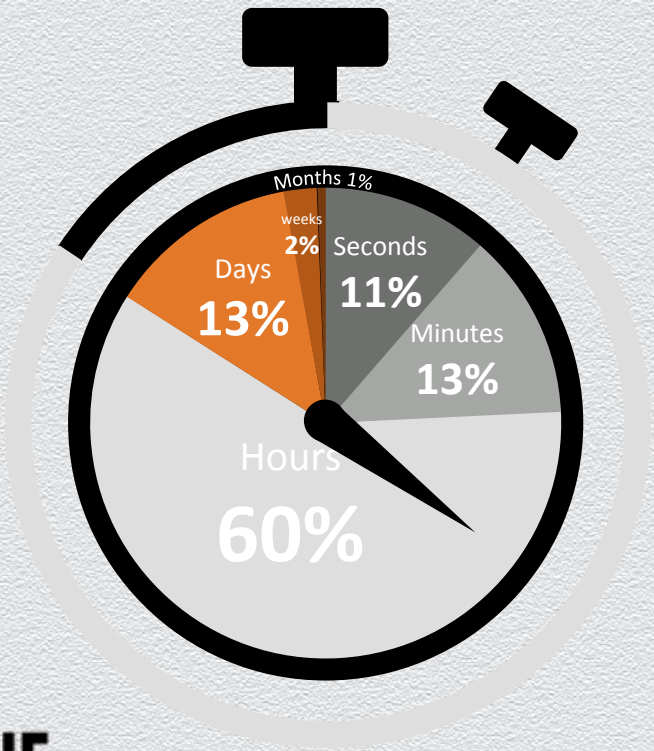
Instead of receiving instructions from an attacker-operated command-and-control server, the Upatre downloader uses an encrypted SSL connection to download malware directly from compromised web servers.

Post-prevention security gap



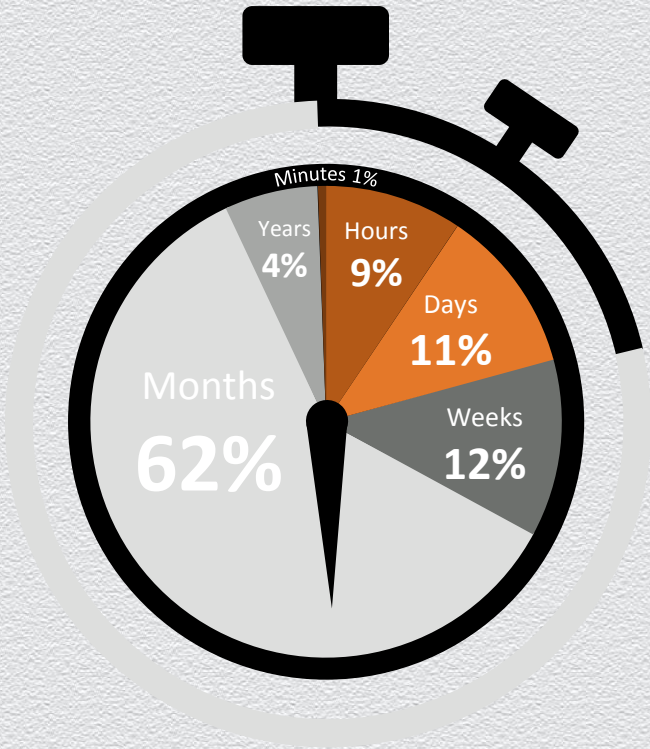
Time and the window of opportunity

Initial Attack to Compromise



84%

Initial Compromise to Discovery



78%

BLUE COAT

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Post-prevention security gap

Percentage of Enterprise IT Security Budgets Allocated to Rapid Response Approaches by 2020.

— Gartner 2013

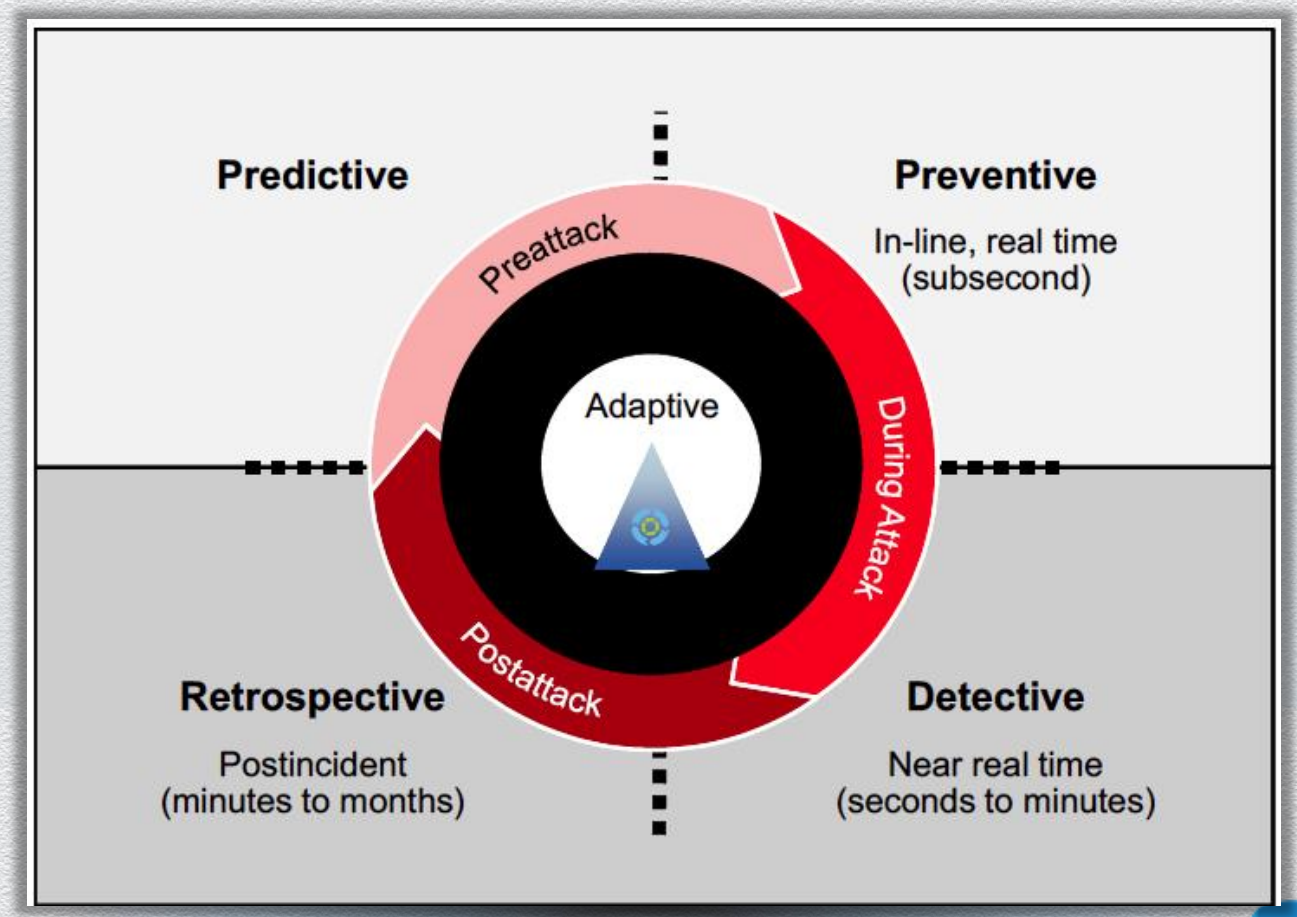
BLUE COAT

#RSAC

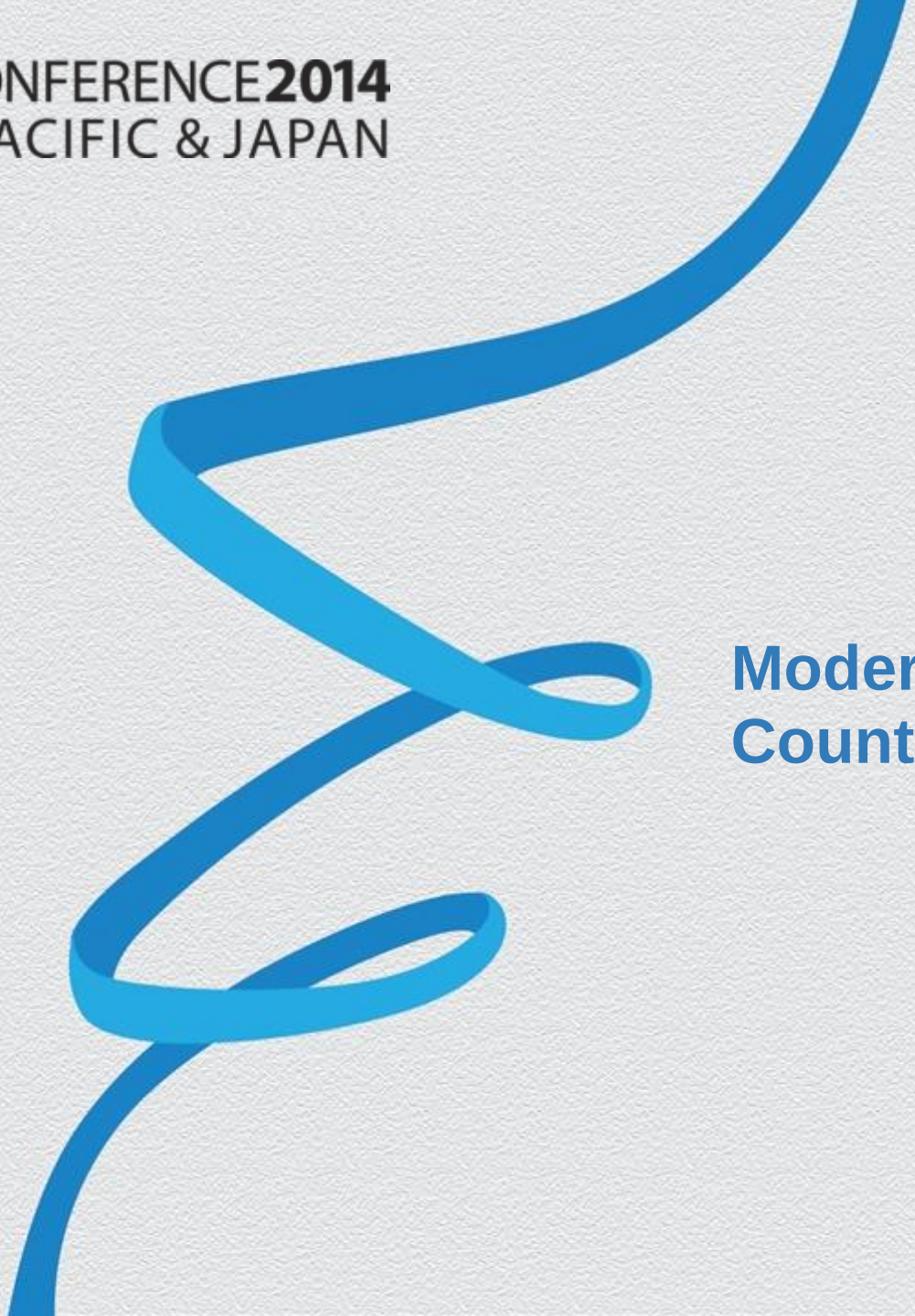
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Mapping the adaptive protection process to the lifecycle of an attack

Gartner



Source: Gartner (February 2014)



Modern Counter-measures

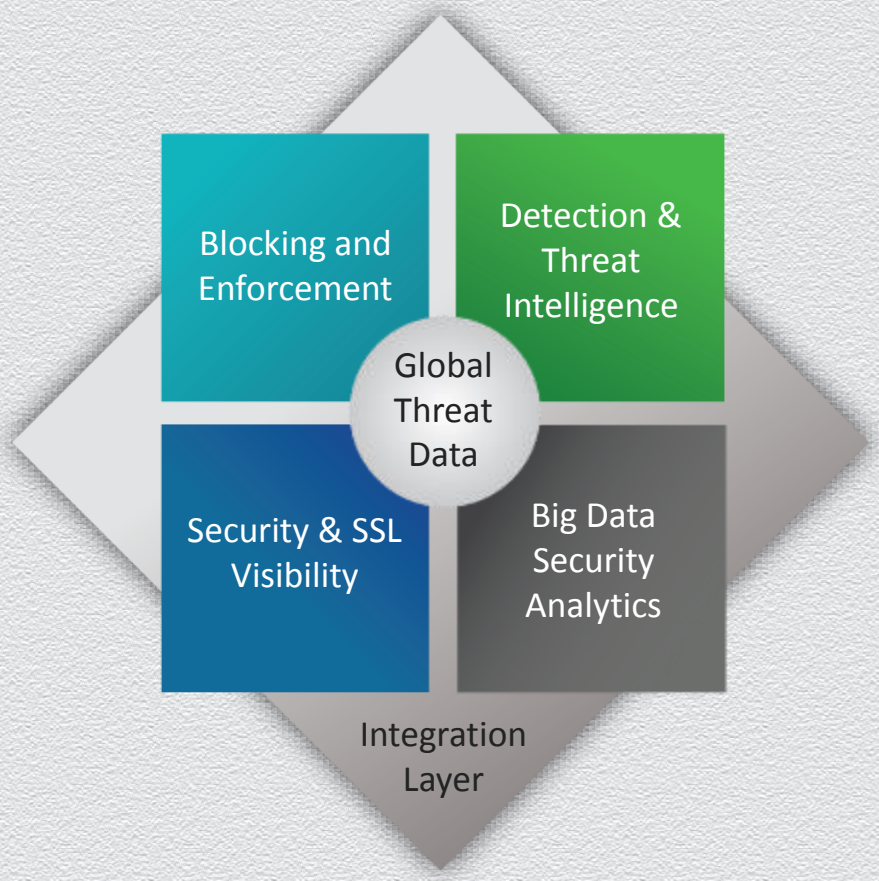
Required technologies for modern advanced threat protection

Complete Web Control
Web Security, Content Analysis, Real-time Blocking

Advanced Malware Detection
White/Blacklists, Sandboxing, Feeds

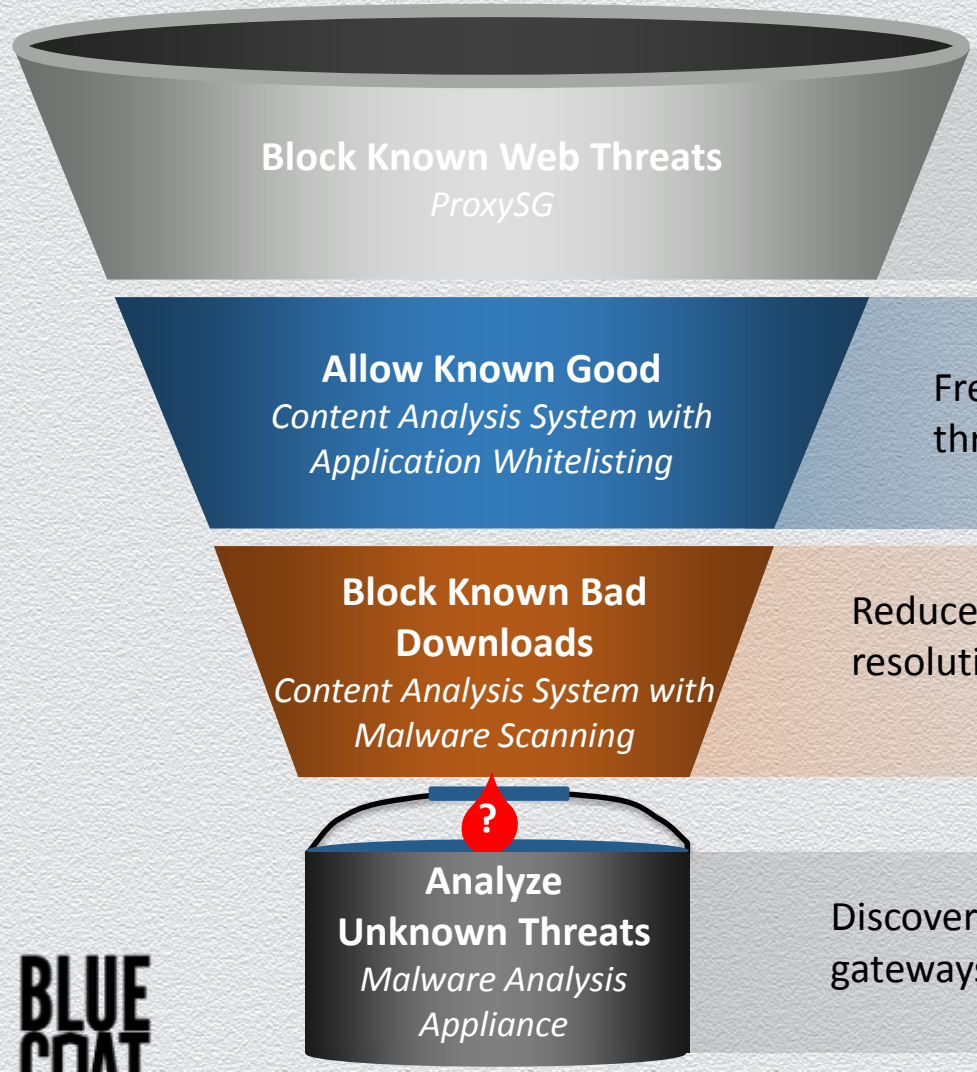
Visual Insight
Context, Real-time Awareness, IOCs, Alerts

Full Packet Capture
Layer 2 – 7 Indexing & Classification



BLUE COAT

Intelligent defense in depth



Block all known sources/malnets and threats before they are on the network

Free up resources to focus on advanced threat analysis

Reduce threats for incident containment and resolution

Discover new threats and then update you gateways

BLUE COAT

#RSAC

RSACONFERENCE2014 ASIA PACIFIC & JAPAN

ADVANCED THREAT PROTECTION
Lifecycle Defense

ADVANCED THREAT PROTECTION LIFECYCLE DEFENSE

BLUE COAT

ADVANCED THREAT PROTECTION
Lifecycle Defense

Ongoing Operations 1 | Incident Containment 2 | Incident Resolution 3

ADVANCED THREAT PROTECTION LIFECYCLE DEFENSE

BLUE COAT

#RSAC

RSA CONFERENCE 2014 ASIA PACIFIC & JAPAN

ADVANCED THREAT PROTECTION
Lifecycle Defense

ADVANCED THREAT PROTECTION LIFECYCLE DEFENSE

BLUE COAT

#RSAC

RSACONFERENCE2014 ASIA PACIFIC & JAPAN

ADVANCED THREAT PROTECTION
Lifecycle Defense

ADVANCED THREAT PROTECTION LIFECYCLE DEFENSE

BLUE COAT

#RSAC

RSACONFERENCE2014 ASIA PACIFIC & JAPAN

Real World Results
Benefit of Lifecycle Defense

Global Financial Enterprise

- 243.21 Billion attempts to access websites
- 793.09 Million attempts to access known malicious sites blocked by SWG
- 89,192 Malicious files blocked by network perimeter antimalware

BLUE COAT

Encrypted traffic management

Policy Based SSL Visibility

Granular Policy Management

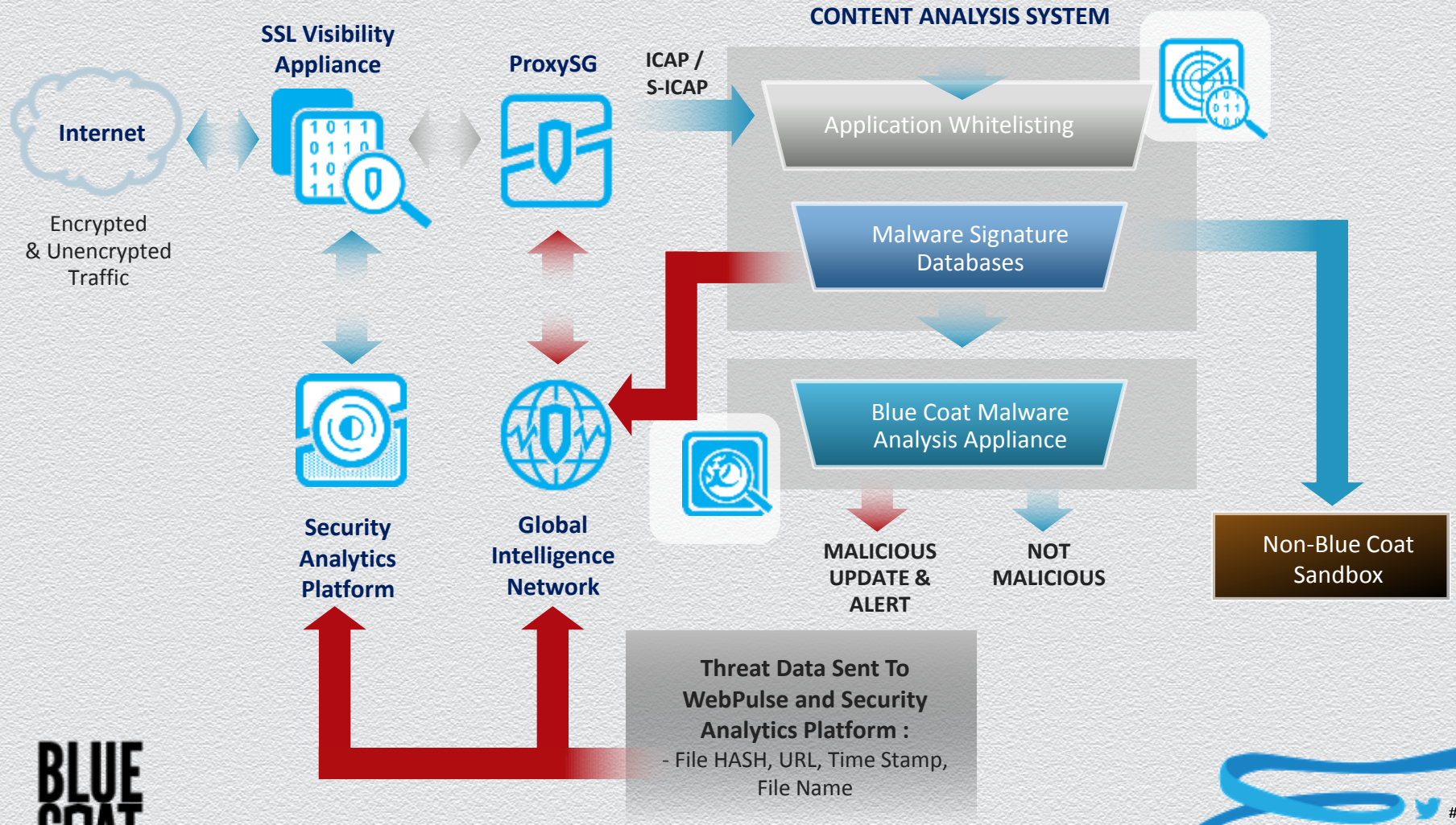
Feed Multiple Security Systems

Industry-leading Performance

Full visibility into encrypted traffic and threats

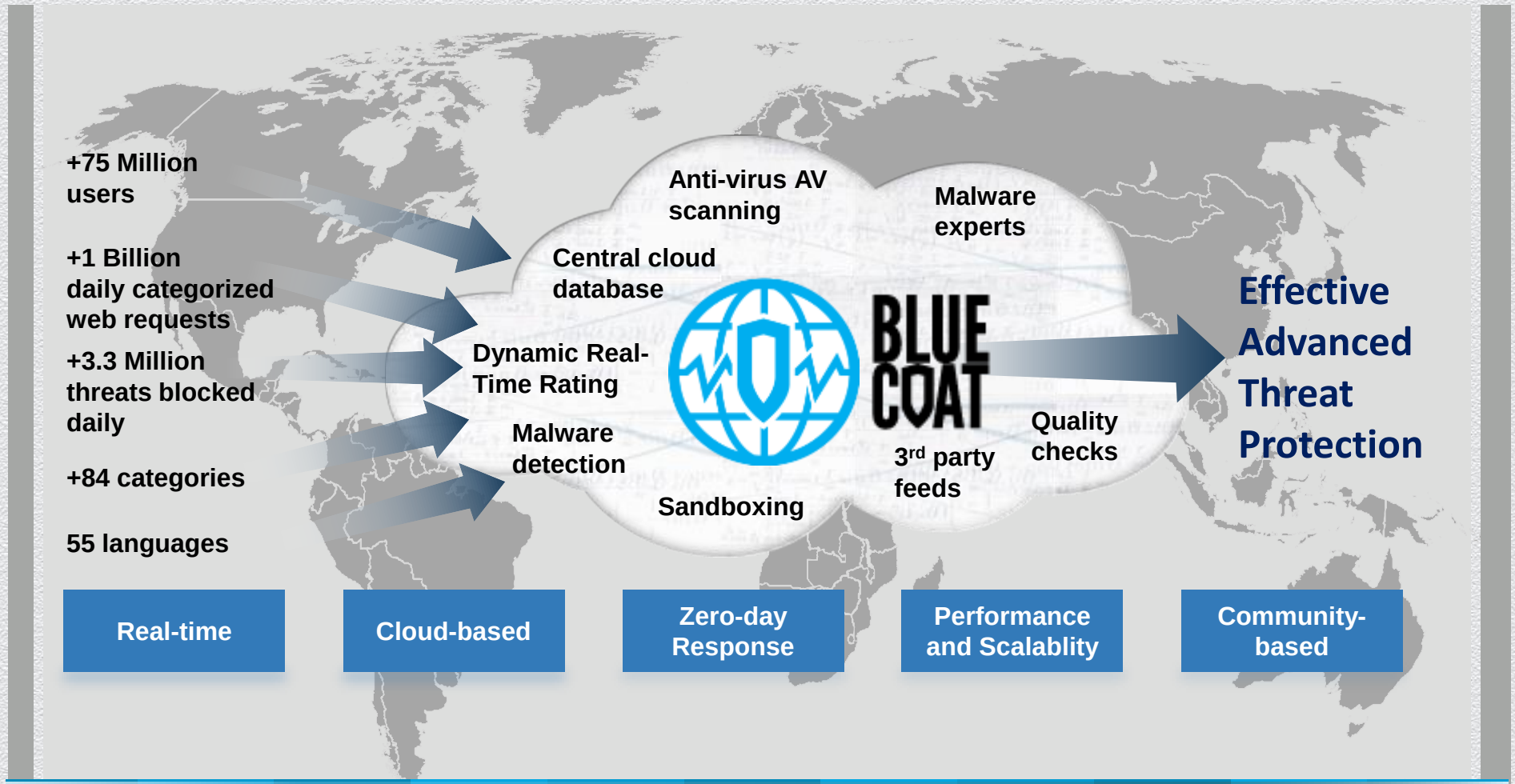
BLUE COAT

Advanced Threat Protection
File Analysis



BLUE COAT

Global intelligence network



Blocks 3.3 million threats per day

ADVANCED THREAT PROTECTION
Lifecycle Defense

Known threats blocked at gateway

Increased system performance through fewer malware scans

Fewer threats to contain and resolve

More robust threat analysis with fewer false positives

BLUE COAT

SECURITY IS ABOUT WHAT YOU MAKE POSSIBLE.

BLUE COAT

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

What we see

SESSION ID: SPO-T11

Mark Hofman

Principal Consultant / Certified Instructor
Shearwater / SANS
@markhofman

Anatomy of an attack

- Reconnaissance
- Delivery/Infiltration
- Code execution
- Network Propagation
- Data Exfiltration

Nothing New Here

BLUE COAT

Reconnaissance

- Two approaches

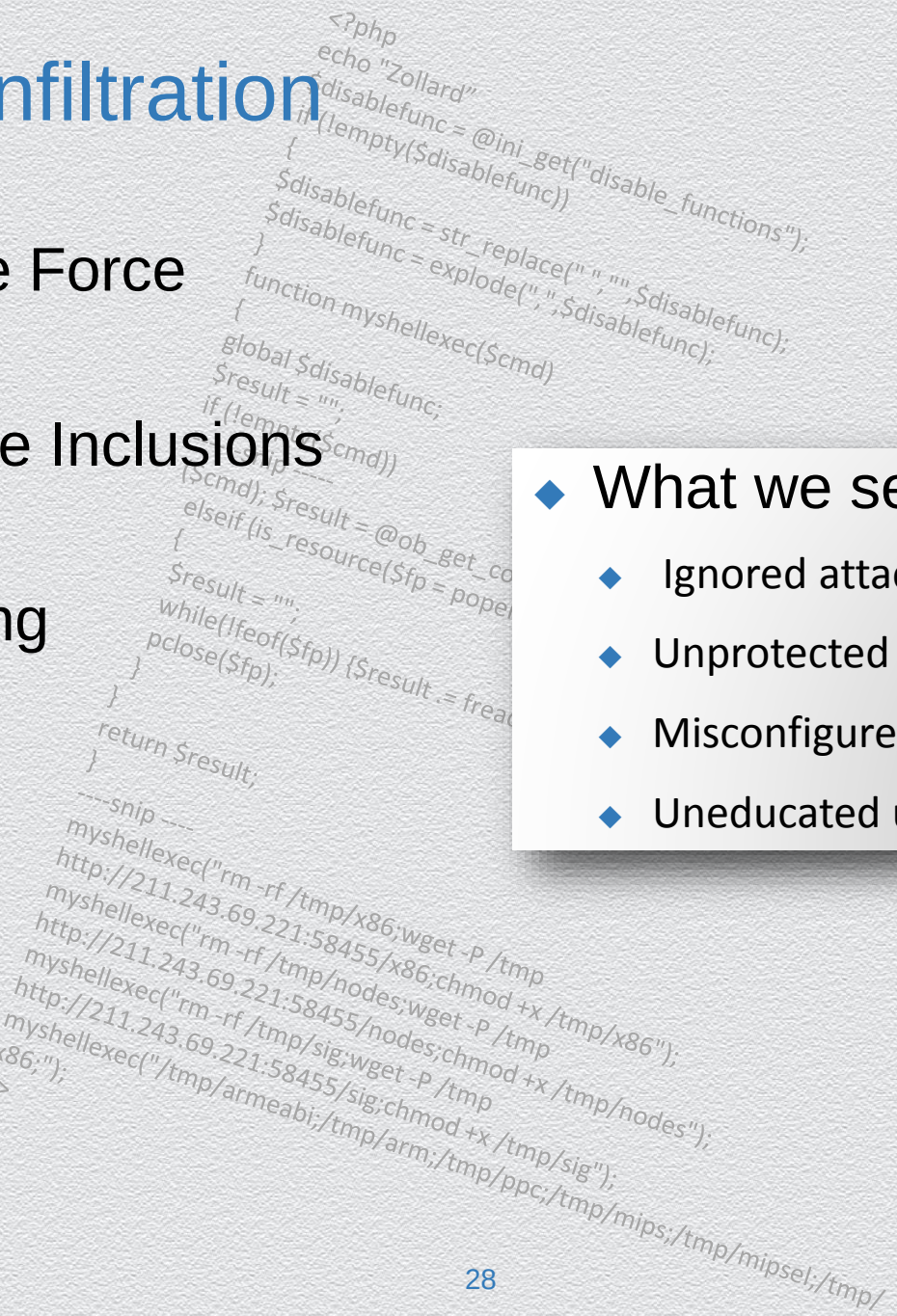
- Sources
  - Google
  - Social Media
    - Linkedin
    - Facebook
    - etc.

- What we see
  - To much personal information
  - Corporate “sensitive” data published
  - No visibility on perimeter or internal network

BLUE COAT

Delivery/Infiltration

- SSH Brute Force
- Remote file Inclusions
- Malvertising
- Drive By
- Phishing

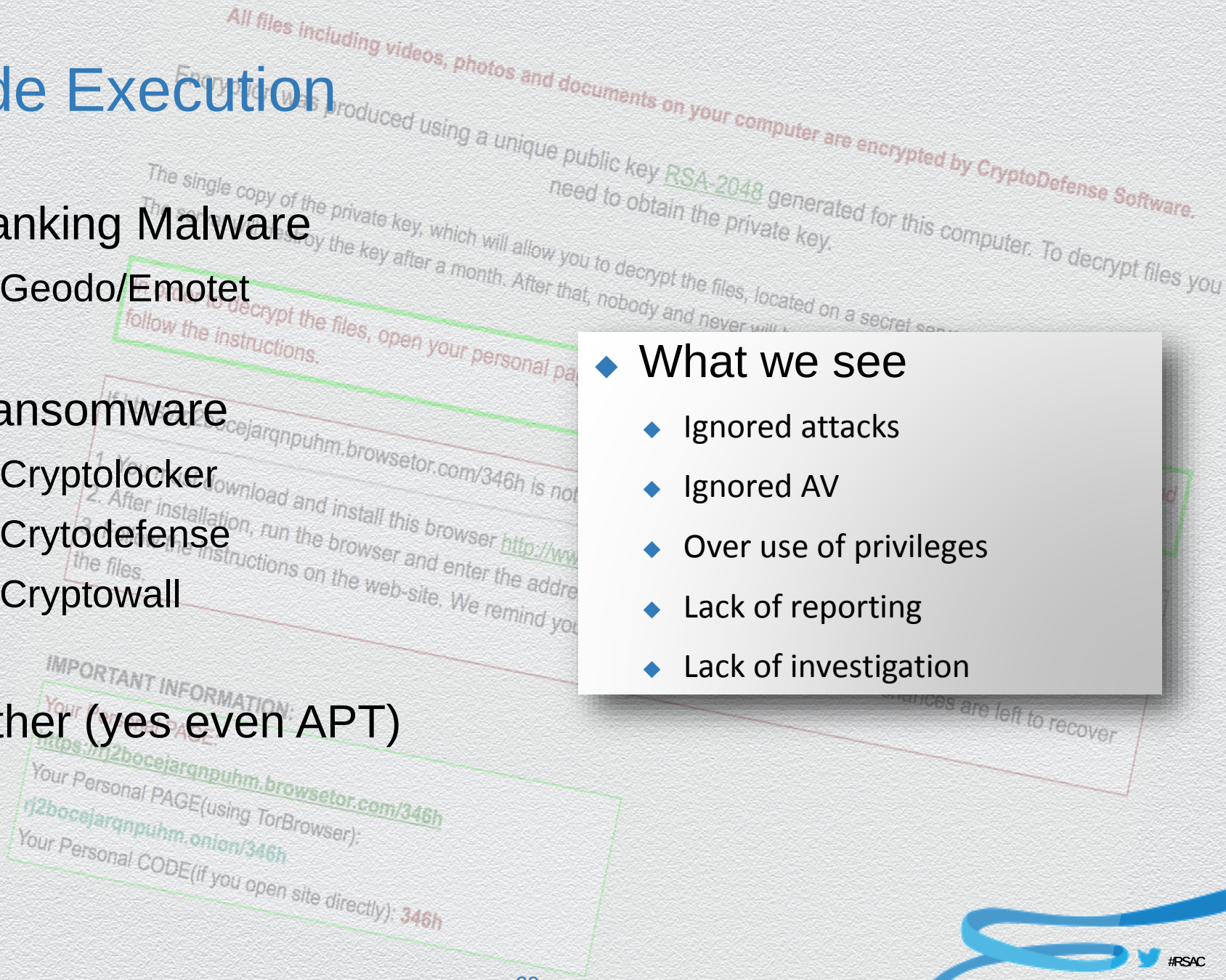


- What we see
  - Ignored attacks
  - Unprotected paths
  - Misconfigured solutions
  - Uneducated users

Code Execution

- Banking Malware
  - Geodo/Emotet
- Ransomware
  - Cryptolocker
  - Crytodefense
  - Cryptowall
- Other (yes even APT)

- What we see
  - Ignored attacks
  - Ignored AV
  - Over use of privileges
  - Lack of reporting
  - Lack of investigation



Network Propagation

- Most networks →

- What we see
  - Ignored attacks
  - Unpatched systems
  - Access issues
  - Management “tools”

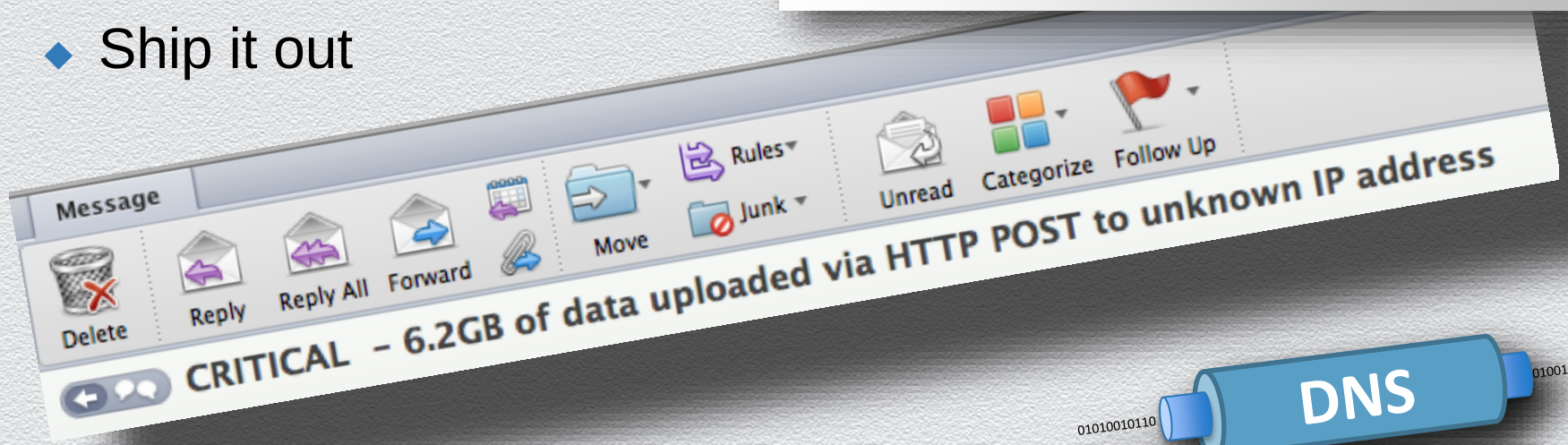
- Use credentials to
- Use vulnerabilities
- Use installed tools

BLUE COAT

Data Exfiltration

- Identify Interesting Info
- Bundle up
- Ship it out

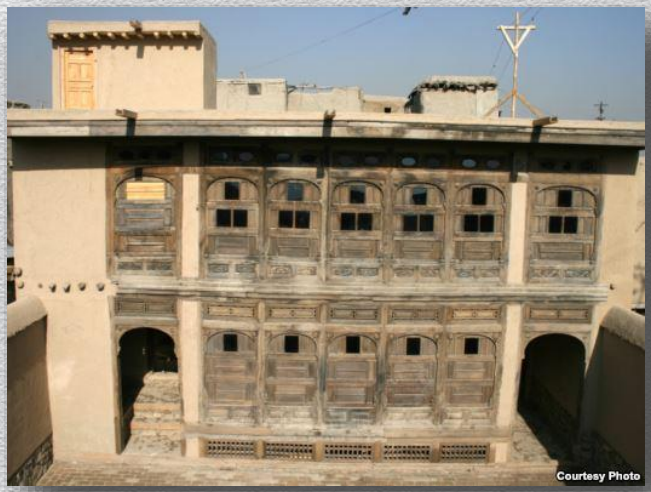
- What we see
  - No knowledge
  - Third party notification
  - Lack of understanding of own network



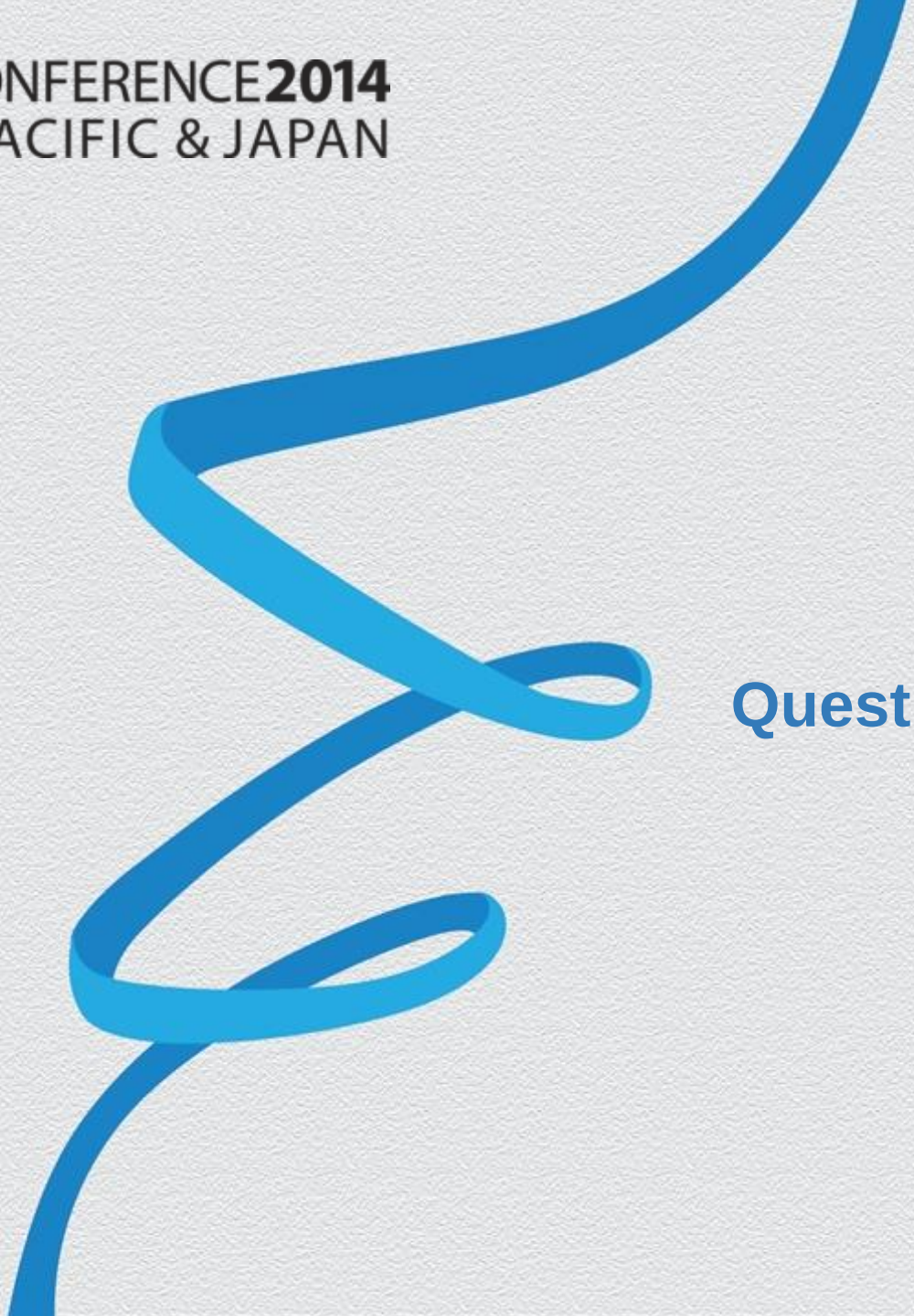
BLUE COAT

What I'd like you to do

- Get your house in order
- Layered controls
  - Technical
    - Content control, IDS/IPS
    - Sand box
    - AV, APP Control
    - Visibility
  - Non technical
    - Policy, Process, People



http://www.rferl.org/content/feature/2187104.html



Questions?

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Thank You!