RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Cybersecurity: An Innovative Approach to Advanced Persistent Threats

SESSION ID: AST1-R01

Brent Conran
Chief Security Officer
McAfee

This is who I am

This is what I do

Student B
The Hack Pack

I used to do this

Then I did this which was really cool

Then I worked for these guys

Until these guys flew airplanes into my building

- which really pissed me off

Then I went to work for these guys

Capitol Hill

Now I work for these guys

I used to be this guy

And now I'm this guy (applause now, please!)

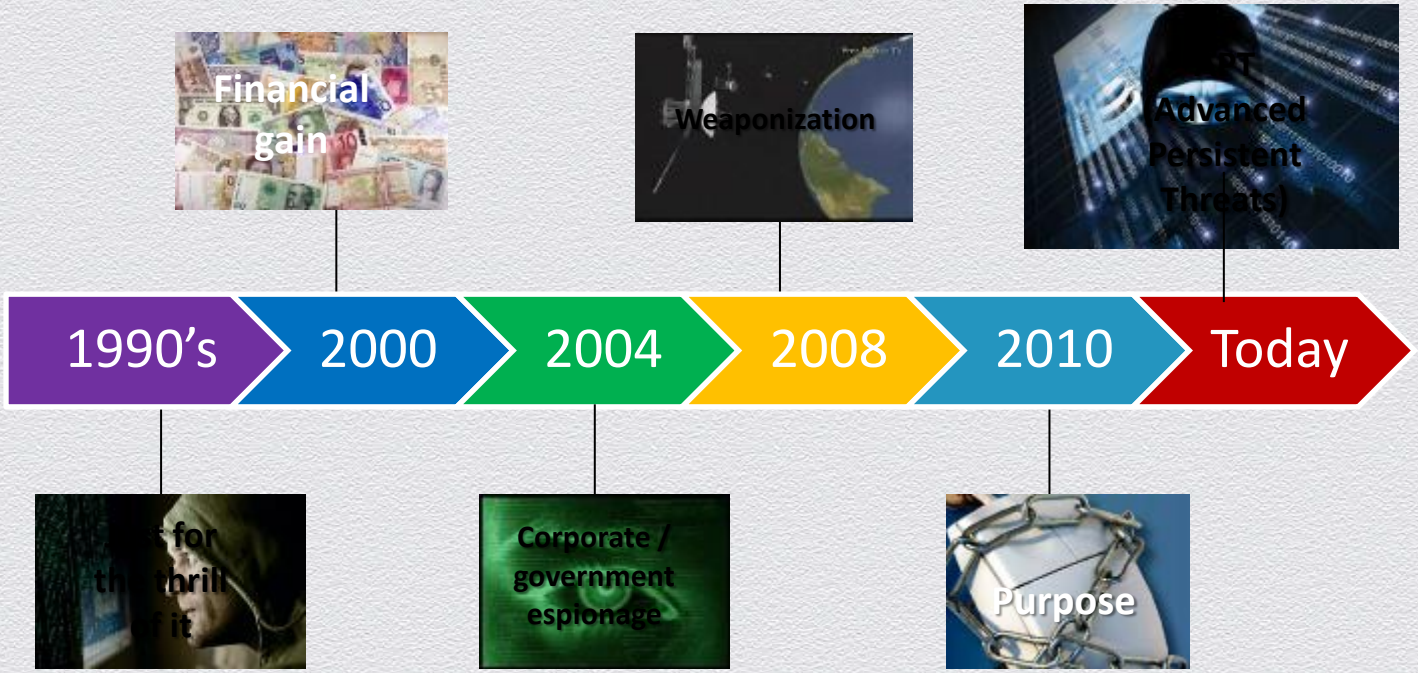
Just moved to Texas and bought a Ford F150 truck

Look a little closer…

Agenda: Advanced Persistent Threats

- How We Got Here
- What Are Advanced Persistent Threats?
- What Should We Be Doing?

How We Got Here



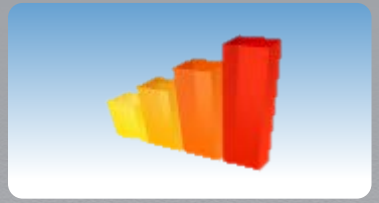
The world is changing

Key trends and drivers of security

Mobility

- Mobile devices
- Social media
- Cloud services
- Nonstandard

The Cloud

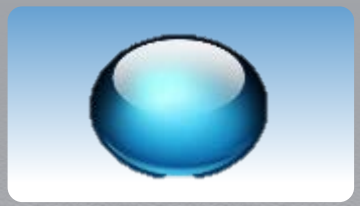


- Global threat intelligence
- Security-as-a-Service

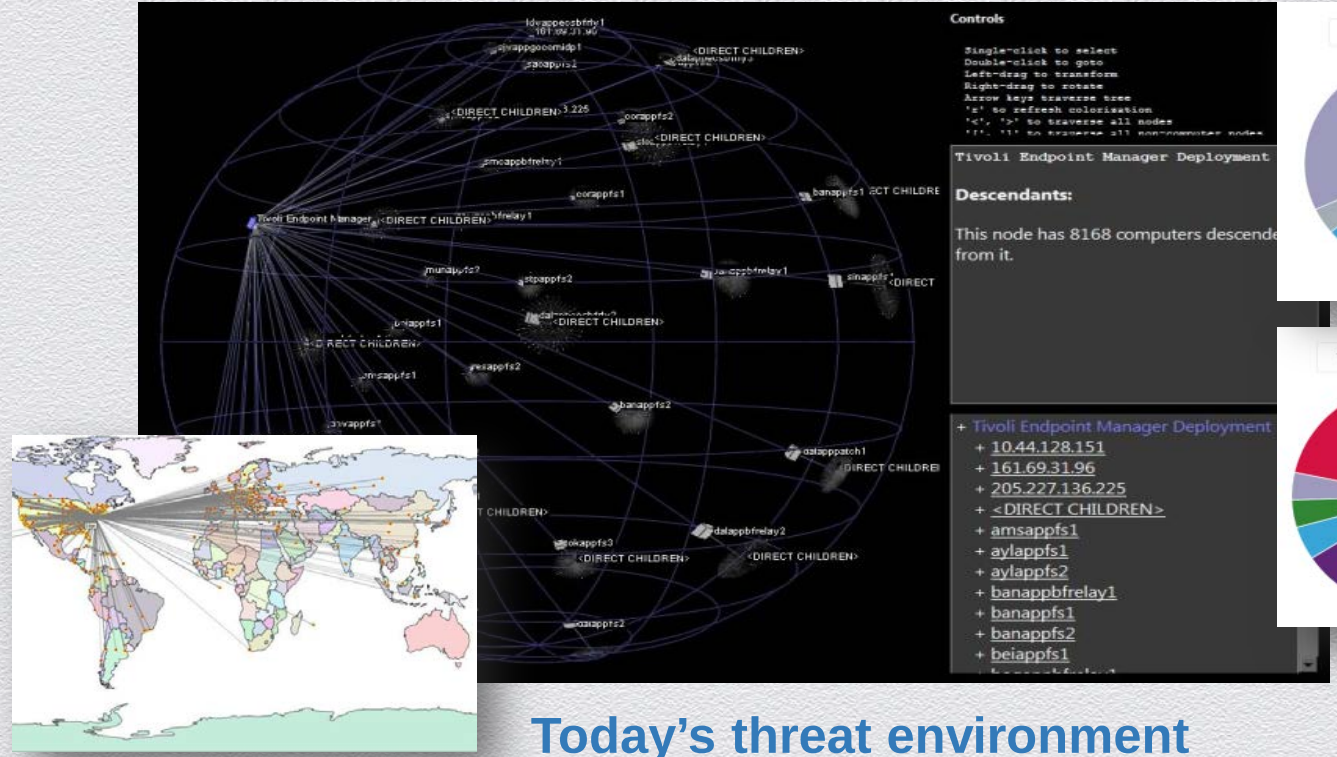
Emerging Threats

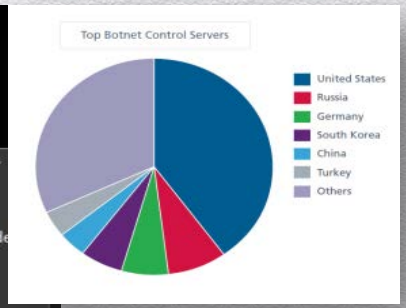
- Decrease in time to exploit
- Targeted attacks
- Advanced persistent threats

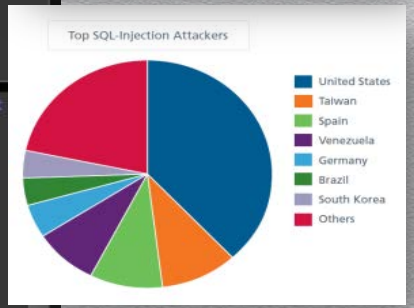
Regulatory and Compliance



- SOX, PCI, EU Privacy
- FISMA
- ISO 27001
- Other regulations







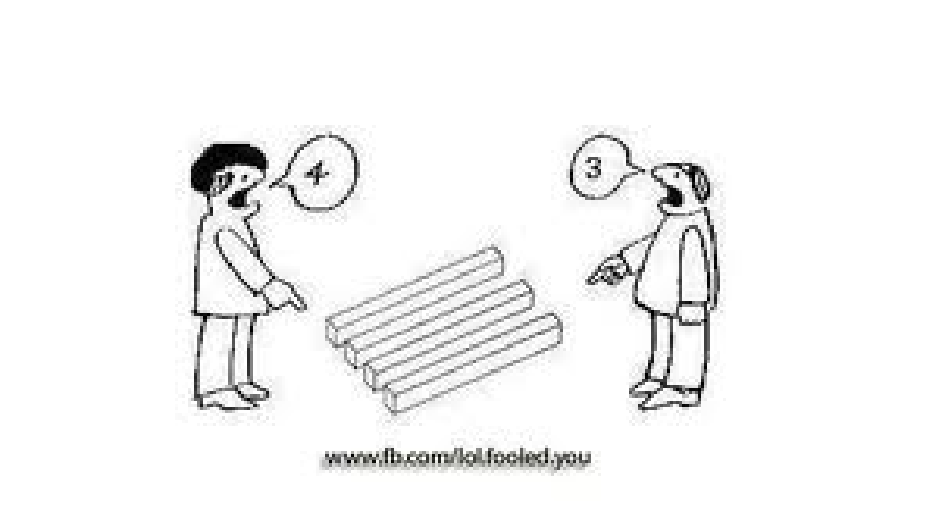
Today's threat environment

- Security Architecture Design & Implementation
- Firewall Protection at Perimeter
- DMZ (single tier) for Internet facing services
- VPN for Remote Access
- Two-Factor Authentication
- 24x7x365 IDS monitoring
- Monthly vulnerability scanning
- Comprehensive patching and anti-virus program
- SPAM filtering
- A well-trained internal security team

Typical Security Office Activities

What are Advanced Persistent Threats?

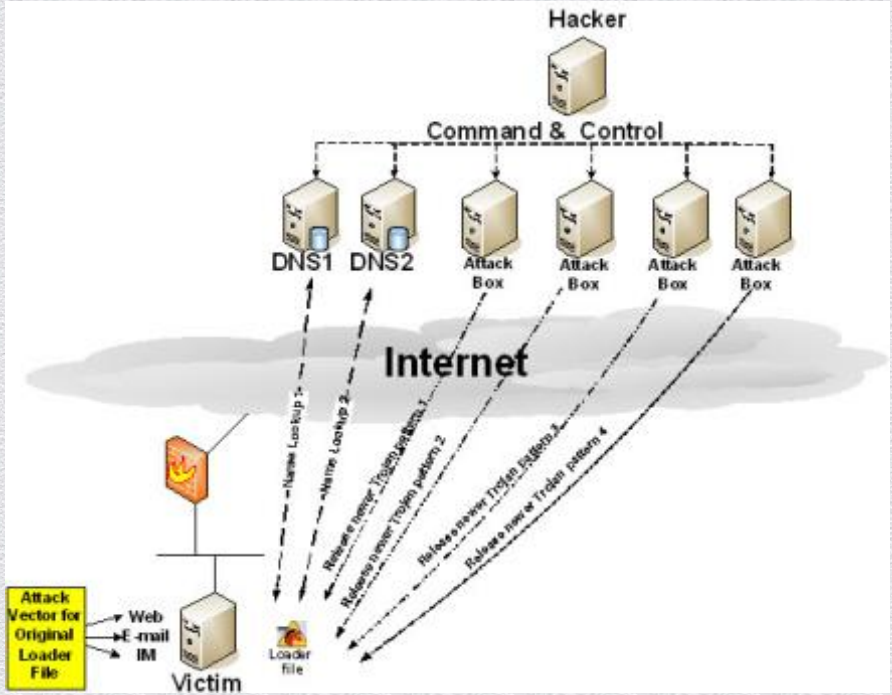
What is Advanced Persistent Threat?



Advanced Persistent Threat is not normal malware. It's a group of highly-skilled, determined actors who are financed to go after intellectual property or commit espionage.

- There's a language barrier
- We see the same thing differently

An example



- Compromise several internal hosts
  - Using unknown malicious code
  - Install user and kernel mode root kits
  - Data mining tools
- Find desktop systems of key users for compromise
- Deploy key loggers widely
- Target corporate executives & key users
- Infiltrate via home, laptop systems and mobile devices
- Copy *.data, compress, encrypt and send
- Go to sleep, set a schedule

What Should We Be Doing?

Build your architecture – and trust it

- Security Architecture Design & Implementation
- Next Gen Firewall Protection
- DMZ (multiple tier) for Internet-facing services
- VPN for Remote Access
- Authentication Framework
- NetFlow
- Wireless Umbrella
- Follow-the-sun Security Operations Center
- Continuous monitoring
- Correct security posture for all devices
- Email filtering
- Web filtering
- Forensics

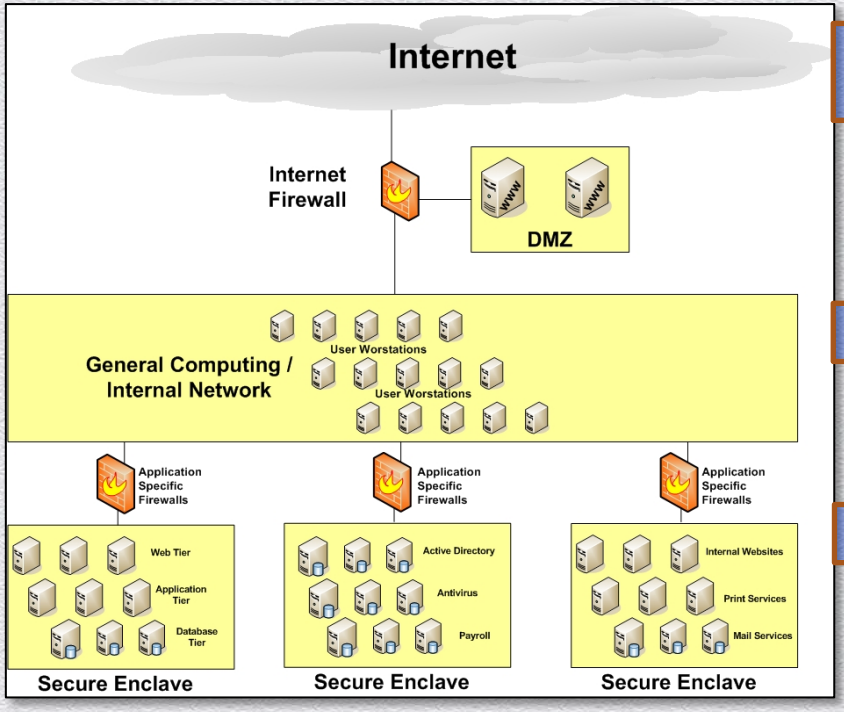
Trust your infrastructure to stop

99%

of threats

Network Architecture

- Your general-purpose network is compromised (Internet2)
- Protect IP in secure enclaves



Everybody on the Outside

Tiered Network

Internal Enclaves

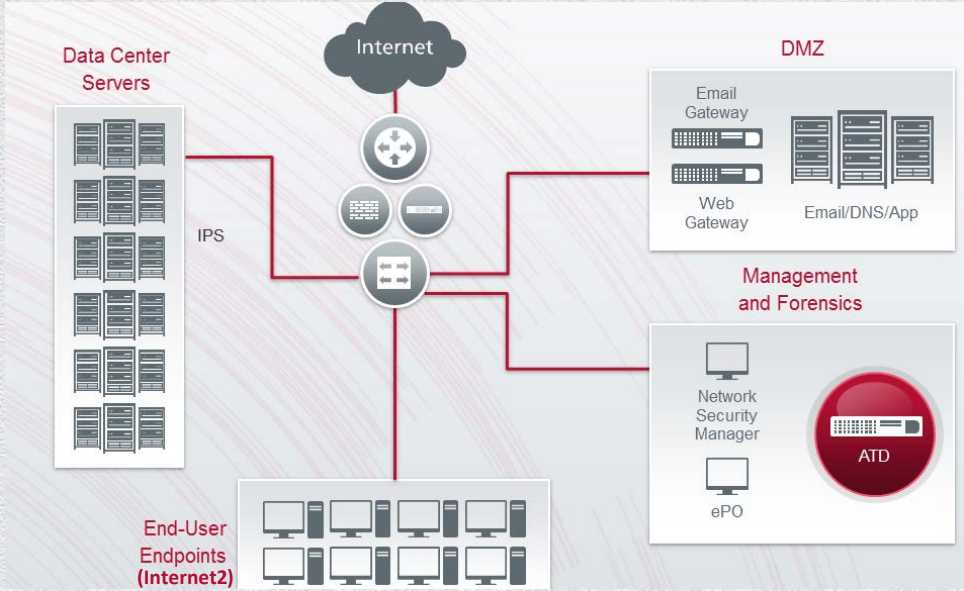
Advanced Threat Defense

Find, freeze, fix

Find: hunt the 1%

Freeze: Freeze threat and prevent infection of other devices

Fix: Identify devices requiring remediation; streamline response across all endpoints



Why it's important

Integrated solutions combining network and endpoint-level visibility and controls are the best way to combat targeted attacks and quickly enable remediation

Volume

- 75 Billion Malware Reputation Queries/Month
- 20 Billion Email Reputation Queries/Month
- 2 Billion IP Population Queries/Month
- 300 Million IPS Attacks/Month
- 100 Million IP Port Reputation Queries/Month
- **100+ BILLION QUERIES**

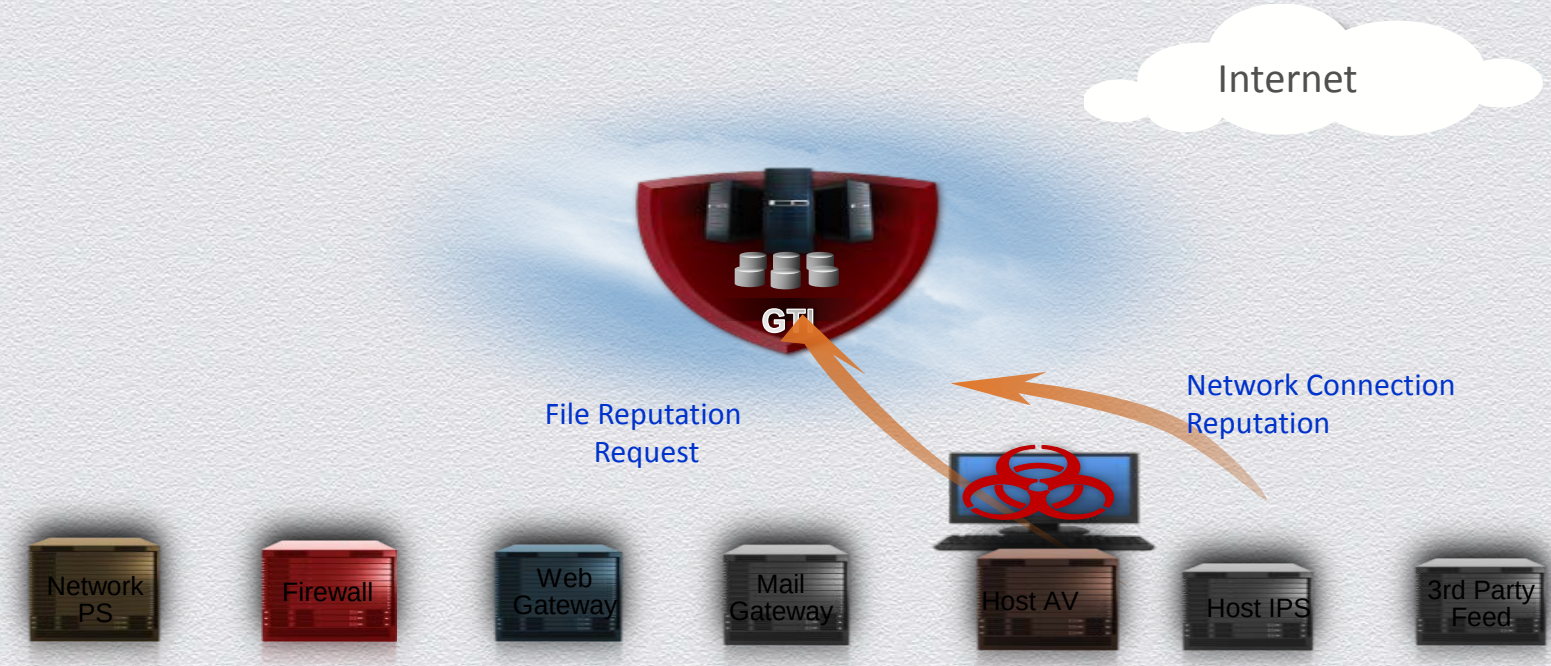
Breadth and Depth

- Malware: 60 Million Endpoints
- Email: 30 Million Nodes
- Web: 45 Million Endpoint and Gateway Users
- Intrusions: 4 Million Nodes
- **100+ MILLION NODES, 120 COUNTRIES**

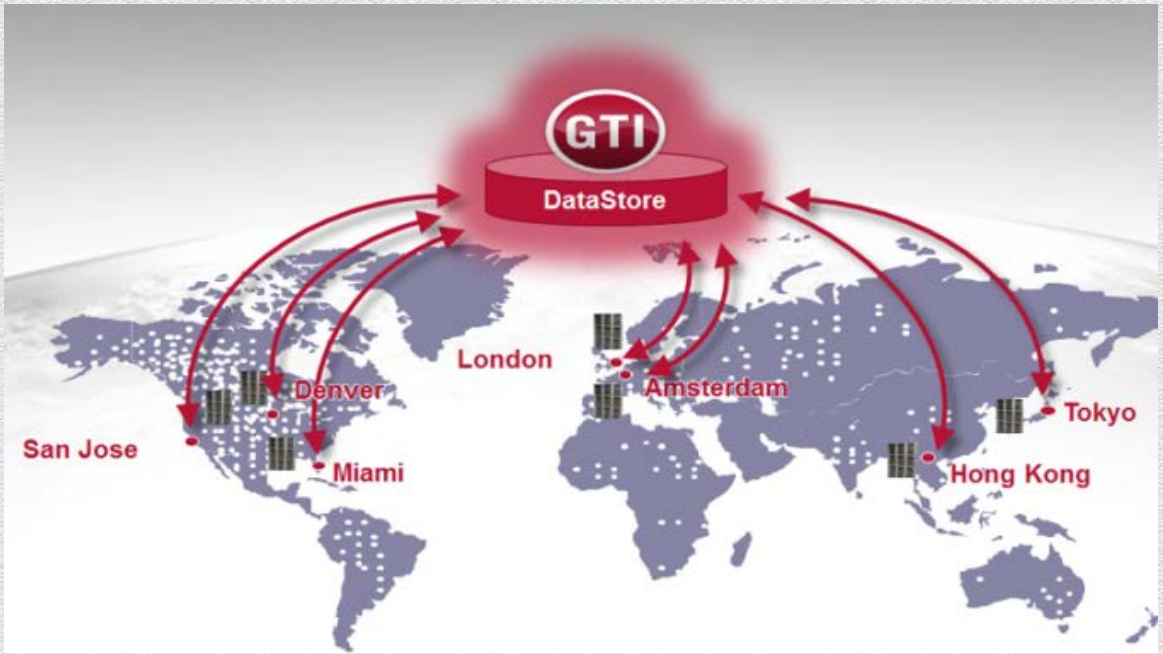
Advanced Threat Defense: Global Threat Intelligence

McAfee An Intel Company

How it works


Internet
GTI
File Reputation Request
Network Connection Reputation
Network PS
Firewall
Web Gateway
Mail Gateway
Host AV
Host IPS
3rd Party Feed

Multi-vector protection



Data Centers Across the Globe

Mobility and the Cloud

- The Challenge
  - No clear boundary between the enterprise and consumer
  - APT becomes easier when lines are blurred
  - Identity and authentication even more important
  - Only host-based security for cloud servers

- Need for Adaptive Authentication
  - Understand you, your device, your location
  - Challenge you with a relevant set of credentials
  - Trust calculation changes based on location, device – and what you are trying to access
- Need Encryption

Summary

- The world has changed, and threats are becoming more complex
- APT has emerged as a different kind of threat
- Need to redesign and re-engineer your architecture (culture): trust your infrastructure, take your warfighters off the fence and turn them into hunters
- Authentication frameworks and encryption will become more important, as mobility accelerates and we move to fat clouds and thin clients
- Keep score with the bad guys when you play the game
- Remember: this is a marathon, not a sprint

Questions

Does anyone have any questions for my answers?

- Henry Kissinger