



Combating Modern Security Threats

Mike Ruiz

Systems Engineer

Disclosure:

Mike is a Senior Systems Engineer at zscaler,
the largest
global internet security service provider.

Recent Major Data Breaches



2015 Breaches (So Far)

2014 Breaches Reported



What are security threats today?

- Wyndam Hotel Group: \$5B in Rev, 33k employees
 - Fined by the FTC for inadequate protection of data.
 - 500,000 Credit Card Numbers stolen, \$10.6M in Fraud Losses
 - Caused by malware on Wyndam Employee Computers
 - Happened Three times

What are security threats today?

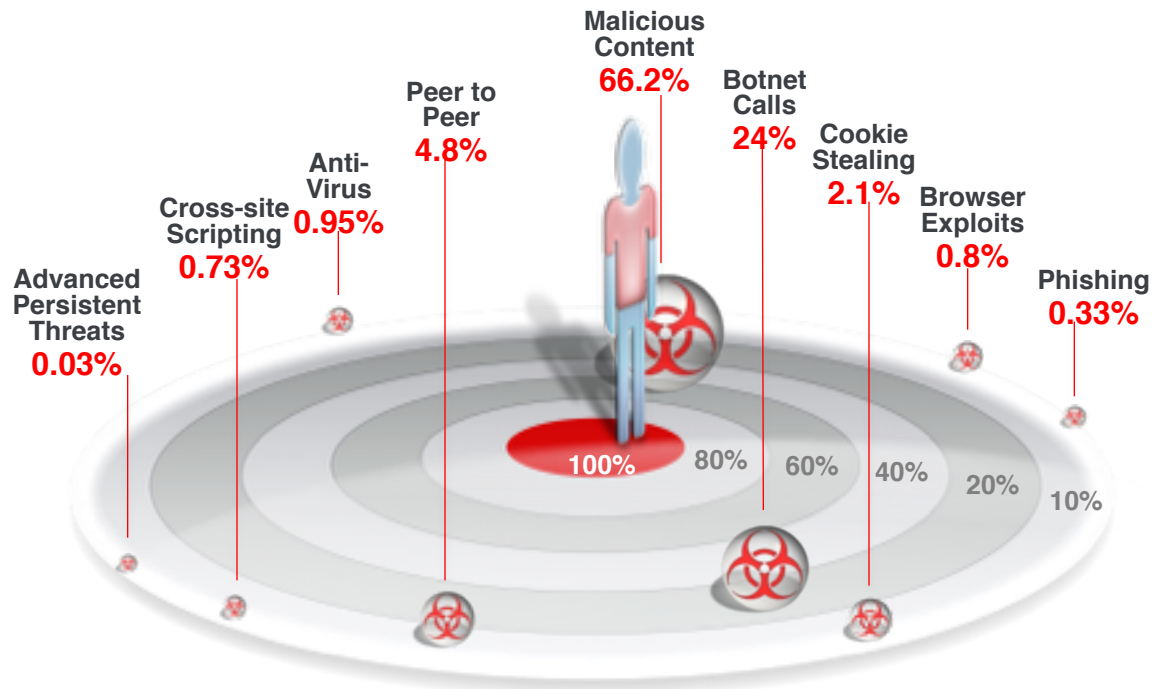
- Target Corporation, \$72B in Rev, 347k employees
 - 11GB of data stolen, affecting 110M people
 - Undetected for three weeks despite advanced security systems
 - Hackers phished a 3rd party contactor outside Target perimeter
 - Gained access to servers when the contractor entered target network

- <https://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/>

Security threats have evolved

- Server Targets
- Worms
- Bots and RATs
- Malicious Code
- User Focused
 - Via Flash, APK, Office Documents, PDF, JPG, etc.

Attacks are broader, deeper and more sophisticated



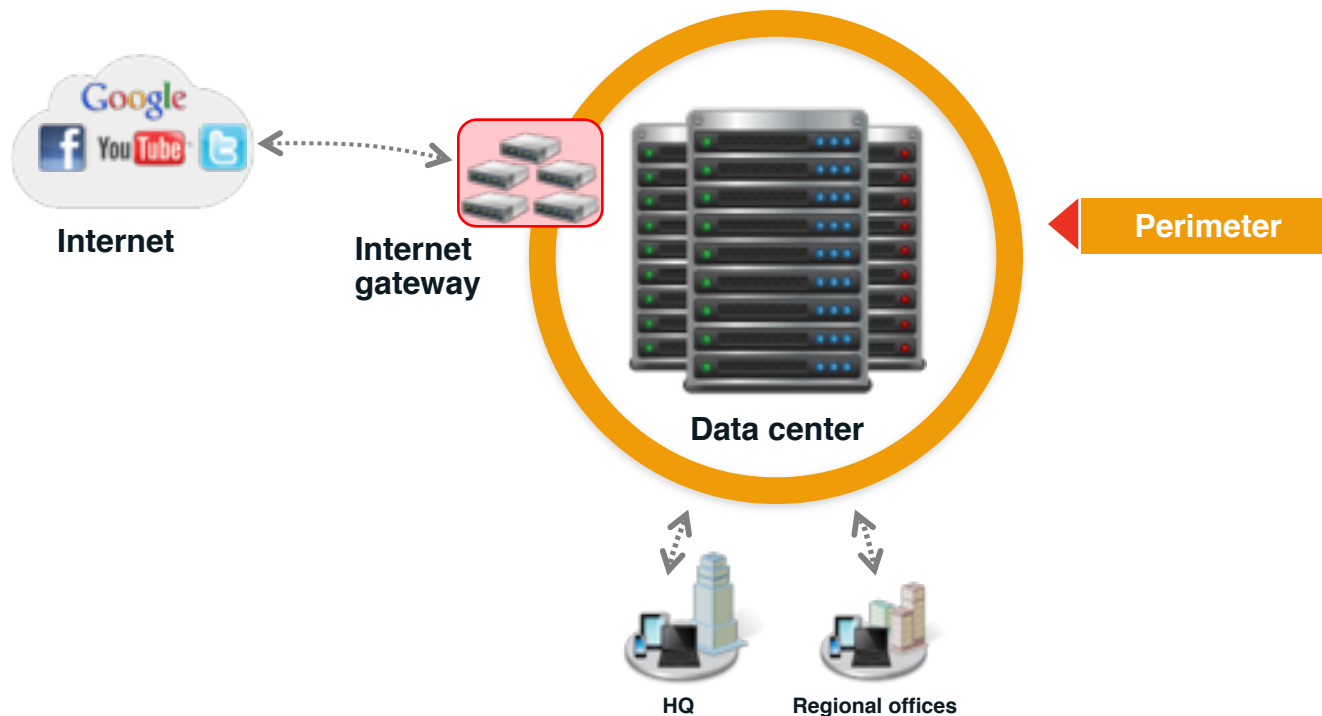
Attacks span multiple vectors – only security platforms can see this

Why have threats evolved?

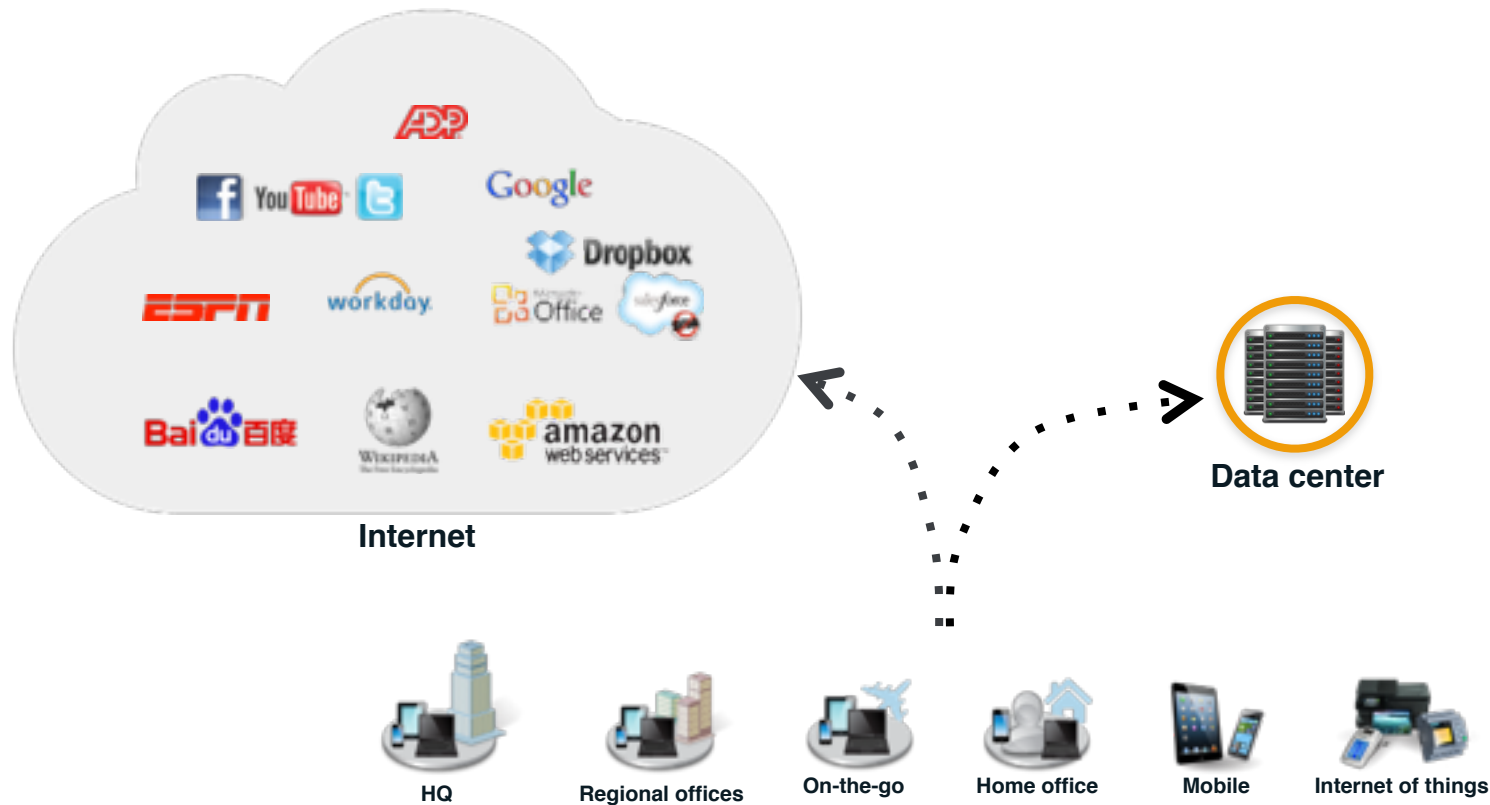
- Endpoint AV/AS
- Endpoint firewalls
- Patch provisioning processes
- Sandboxing technologies
- But really, the perimeter and point solutions are leaky



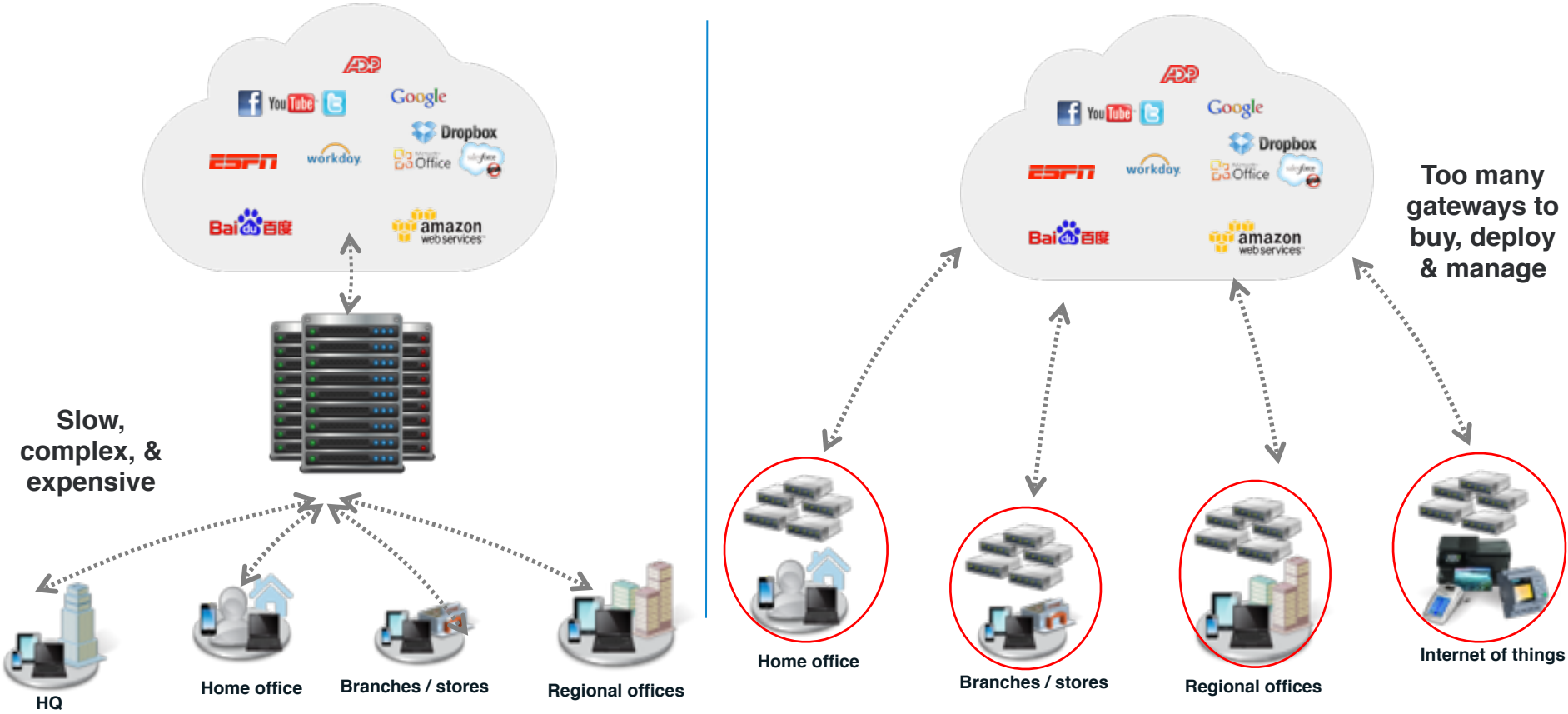
Traditionally organizations secured their perimeter with security appliances in the data center



But with the new world of IT, there is no perimeter anymore



Security appliances: Approach to the new world of IT



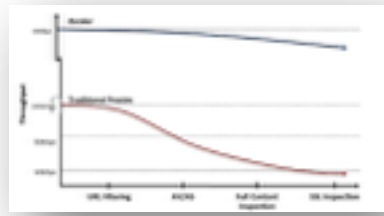
Today's approaches and solutions are failing to protect you



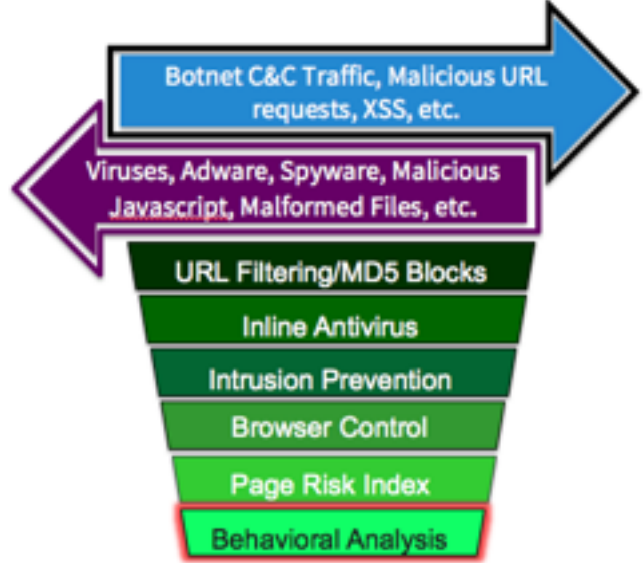
Security gaps



Coverage gaps



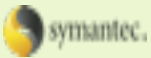
Performance limits



You MUST Scan Everything, Always.



Protect the device



MDM, Device encryption, AV

Protect everything else



Regional offices



Branches / stores



Factories



HQ



On-the-go



Internet of things

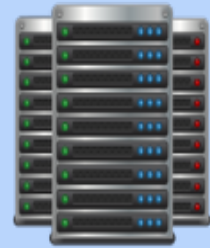


Mobile



Home office

Protect the data center



FW/IPS, WAF, DDOS, App sec.



Thank You

HOW SAFE ARE YOU?

Find out at:

<http://securitypreview.zscaler.com>