

**invincea**<sup>TM</sup>

*Breaking the Security  
Insanity Cycle*

**Anup K. Ghosh, PhD  
Founder & CEO  
Invincea, Inc**

**[anup@invincea.com](mailto:anup@invincea.com)**

*Confidential and Proprietary*

---

# Information Security – Caught in a Vortex

---

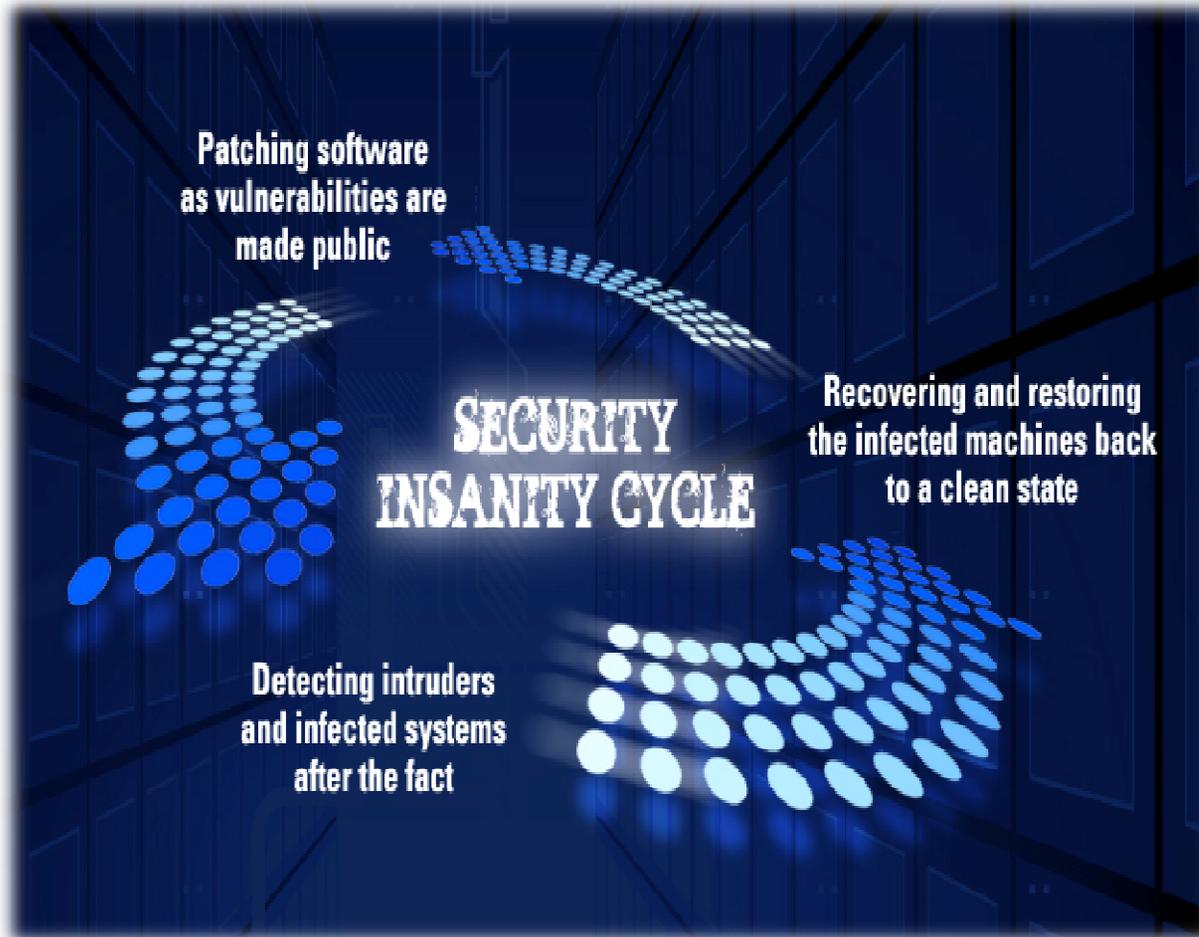


- The adversaries are winning - despite billions in investments over past 20 years
- Treating symptoms not disease
- Servicing problems not solving them
- Chasing our tails while adversaries innovate
- Slinging mud and calling FUD instead of rallying to the common cause

---

# *We Must Break the Security Insanity Cycle*

---

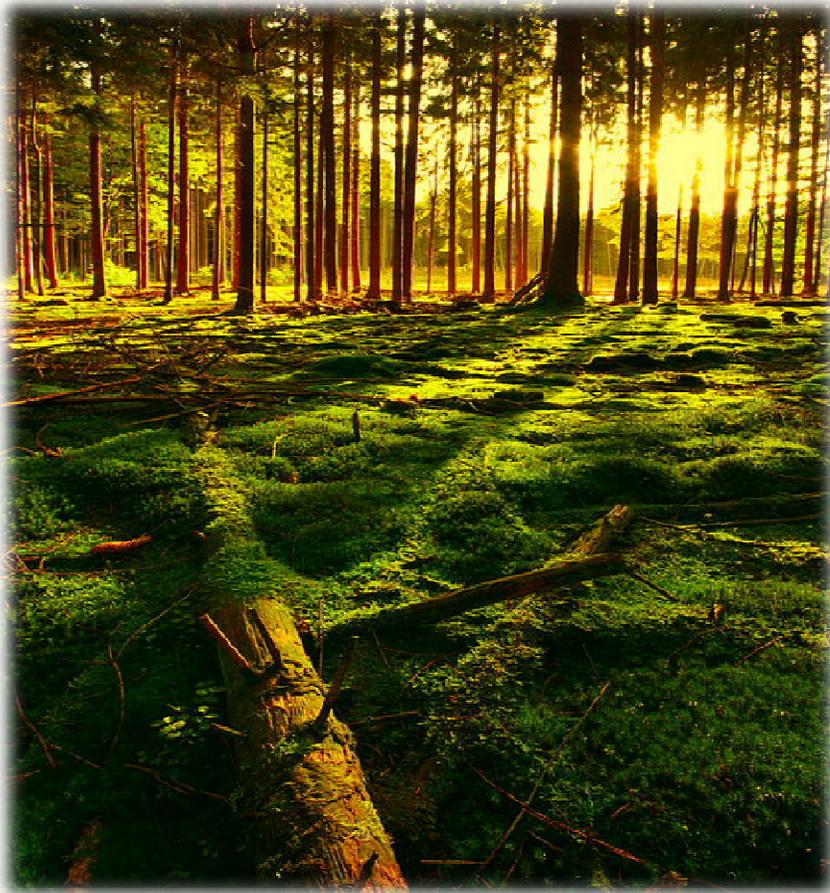


- Wash, rinse, repeat security
- Finding out Tuesday that we were pwned on Monday
- Whack-a-mole problem resolution
- Glorify those that break – drastically undervalue innovation

---

# The Problem is MASSIVE – No One Immune

---



- 2011 so far...
    - “White House” eCard
    - OddJob
    - HBGary Federal
    - Night Dragon
    - Tatanga
    - London Stock Exchange Website
    - French Finance Ministry
    - Dupont, J&J, GE
    - DroidDream
    - Charlieware
    - Nasdaq
    - Office of Australian Prime Minister
    - Comodo
    - RSA
    - Epsilon
    - LizaMoon
    - Barracuda Networks
    - Oak Ridge National Labs, PNNL
    - Sony
    - Lockheed Martin
    - BAH, ManTech
- ....and today?

---

# The Stakes are Enormous

---



***“We are on the losing end of the largest transfer of wealth through theft and piracy in the history of the planet.”***

Senator Sheldon Whitehouse (D-RI)  
Chair US Senate Select Committee on U.S.  
Cyber Security 2010

---

# The Stakes are Enormous

---



*“It appears that every industry is being victimized by intrusions.”*

Steven Chabinsky  
Deputy Assistant Director – FBI

---

# The Stakes are Enormous

---



***“To Dupont it’s personal...they believe their bad guys are the Chinese who want to leapfrog them in the global marketplace.”***

Leaked HBGary email disclosed in Bloomberg report

“Hackers Strike at Major Companies”

---

# The Stakes are Enormous

---



- Adversaries are growing in number and blurring lines
  - Organized crime making forays into state espionage and corporate IP theft
  - 108 nation states with offensive cyber capabilities – now making forays into corporate IP theft
- GAO - \$50 billion lost in Intellectual Property theft every year
  - British Government - 21 billion pounds
- Competitiveness on the global scale is at the heart of the issue – these aren't cyber-annoyances – these are national security concerns

# A Digital Pandemic?

## Malware is Everywhere and it is Everyone's Problem

- 60,000 new pieces of malware released on a daily basis in Q3 2010 – 4x more than 2007 <sup>(1)</sup>
- 20,000,000+ unique pieces of malware *identified* in 2010 <sup>(2)</sup>
- 139% growth in web-borne malware from 2009 to 2010 <sup>(3)</sup>
- 33% of EU Internet users infected with a virus despite 84% having a/v, anti-spam or firewall in place <sup>(4)</sup>
- 60% of top Google search terms delivered user to malicious sites in first 100 results <sup>(2)</sup>

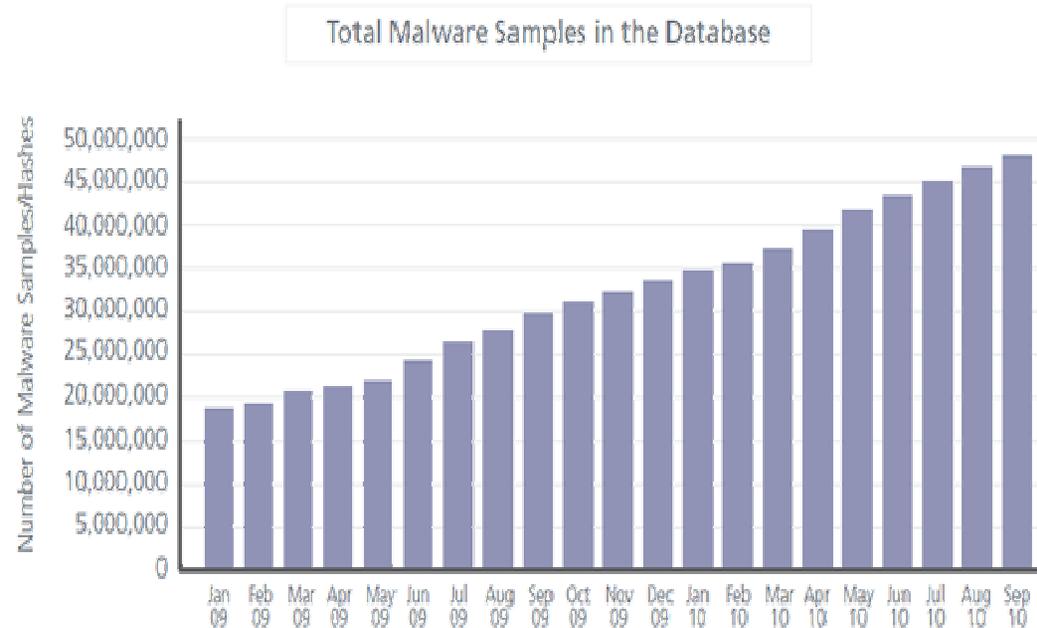
(1) McAfee threat report – November

(2) PandaLabs – December 2010

(3) Cisco Global Threat Report – February 2011

(4) EUROSTAT Report – February 2011

(5) McAfee Threat Report – November 2010



Total count of unique malware (including variants) in the McAfee Labs database.

**Very important note...these are just the pieces that have signatures...**

# Malware Drives Real Cost

## Whack-a-Mole Incident Response

- 4 weeks per investigation
- Anti-remediation battles

## Escalating Support Costs

- Reimaging machines
- Opportunity costs

## Business Downtime

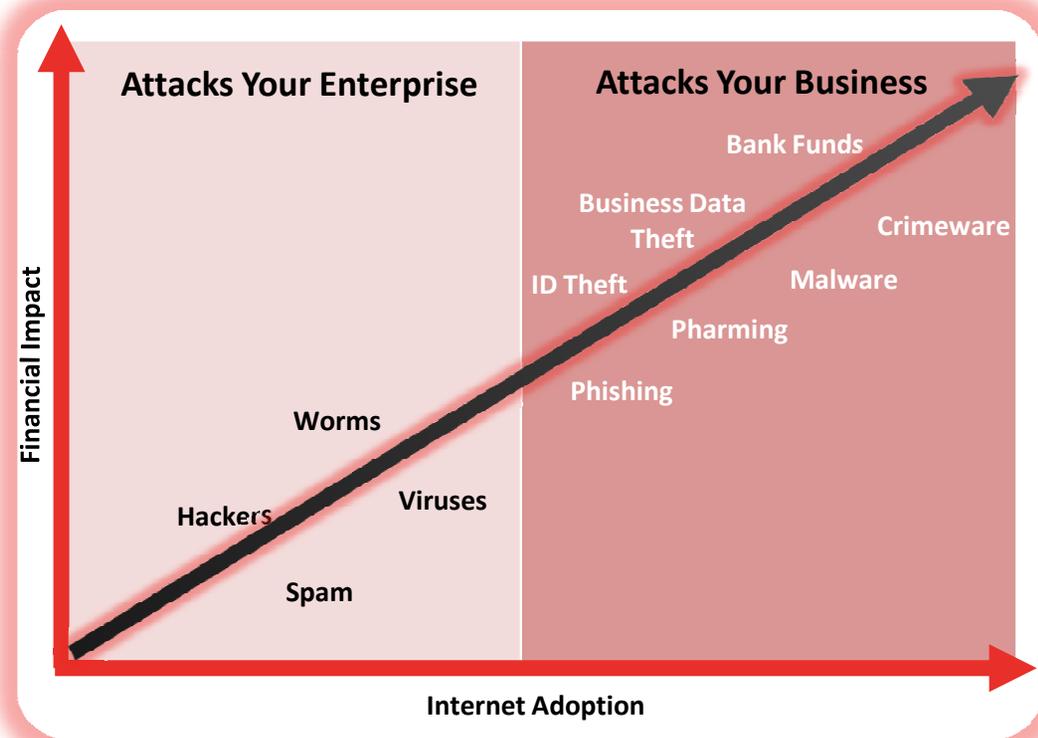
- 65% have been the victim of cybercrime

## Loss of Intellectual Property

- 50% surveyed stated IP was targeted

## Fraud and Legal Expense

- Breach notification and support costs alone could reach millions per incident



**2009 McAfee and Symantec Estimate Global Cost of Computer Crime = \$1 trillion**

*First Annual Cost of Cyber Crime Study, Ponemon Institute July 2010*

# Existing Defenses are Inadequate

## Firewalls

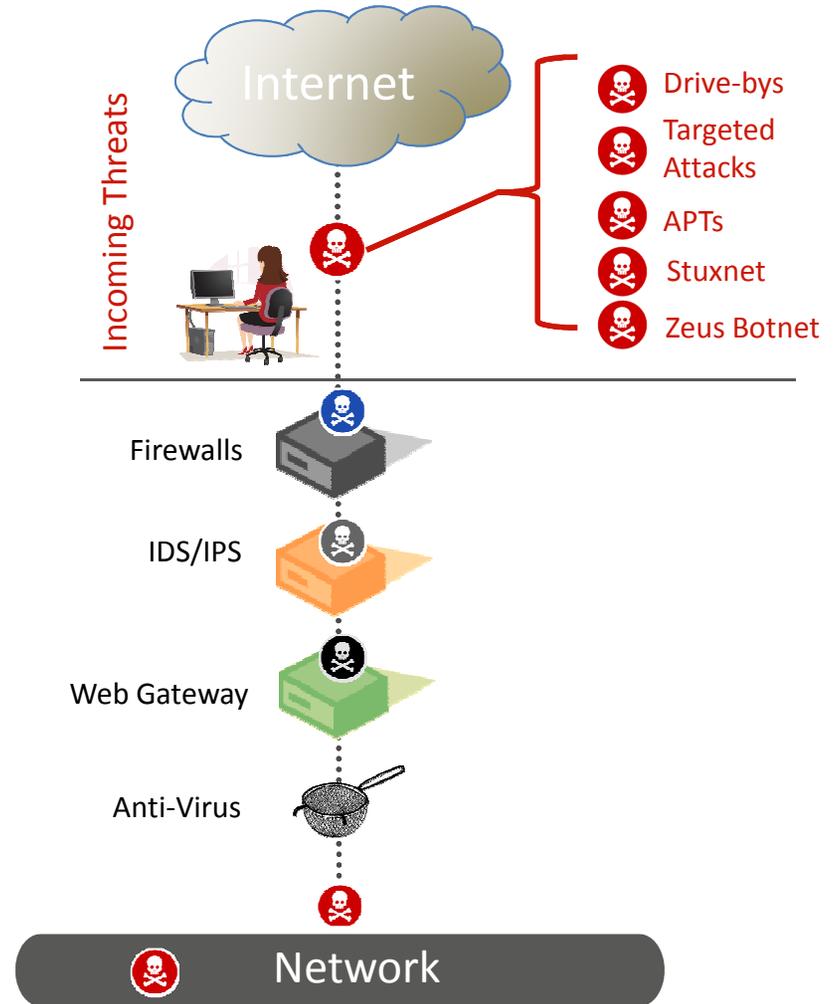
- Perimeter fencing
- Only stops “known bad” url requests

## Network Gateways

- Requires signatures of “known bad”
- Choke-point for Web traffic – scale?
- Requires successful breaches to identify new malware
- Misses malware requiring human interaction

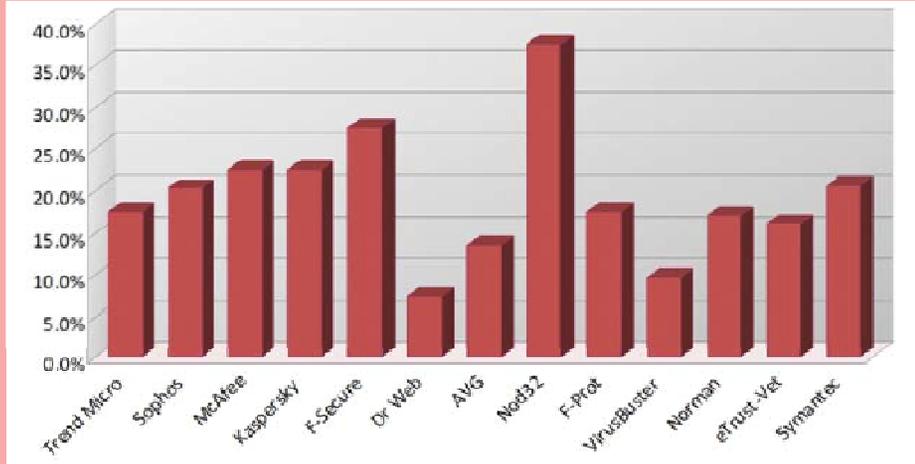
## Anti-virus

- Requires signatures of “known bad”
- Malware built to avoid AV detection
- Signature updates lag by days/weeks



# Independent Studies Reveal the AV Gap

## Day 1 Anti-Virus “Effectiveness”



Average anti-virus detection rate:  
19% “Day 1”  
62% “Day 30”



## Day 30 Anti-Virus “Effectiveness”

	Trend Micro	Sophos	McAfee	Kaspersky	F-Secure	Dr Web	AVG	Nod32	F-Prot	Symantec
Day 1	17%	20%	22%	22%	27%	7%	13%	37%	17%	21%
Day 8	29%	36%	53%	87%	50%	29%	85%	86%	23%	36%
Day 15	32%	75%	85%	91%	59%	33%	92%	88%	34%	43%
Day 22	32%	81%	86%	92%	62%	33%	92%	88%	37%	46%
Day 30	38%	85%	86%	92%	64%	33%	93%	89%	39%	47%

\* Malware Detection Rates for Leading AV Solutions, A Cyveillance Analysis, August 2010

---

# Addressing a Root Cause...

## *The User is an Unwitting Accomplice*

---

- Ubiquitous usage of Internet and PDFs has enabled adversaries to shift tactics
- Full frontal assaults still exist but it is far easier to prey on the psychology of the user
  - Trust in social networks
  - Faith in Internet search engines
  - Trusted sites
  - Spear-phishing
  - Fear mongering



***"I don't know security...but I know what I like.  
Click, click, click..."***

*Stan from Accounting | December 2010*



Your first line of defense is also your weakest link...how many thousands of ~~users~~ *vulnerabilities* are in your network?

---

# Key Statistics Related to Breach

---

## Total Incidents Reported to US-CERT FY 2010

Phishing	56,579	52.7%
Virus/Trojan/Worm/Logic Bomb	11,001	10.2%
Malicious Website	7,971	7.4%
Non Cyber	7,741	7.2%
Policy Violation	6,888	6.4%
Equipment Theft/Loss	5,395	5.0%
Suspicious Network Activity	3,121	2.9%
Attempted Access	2,712	2.5%
Social Engineering	1,571	1.5%
Others	4,460	4.2%
Total	107,439	100%



**According to one of the leading IR providers – 95% of incidents they respond to involve the user**

# A Quick Look at the Spear-Phishing Workflow



## Attacker prepares the phish

- Searching company websites, job postings, corporate communications, news sites, blog sites, social networking sites
- Uses information gathered from previous compromises (i.e. email addresses from Gannett or Epsilon breaches)



## Hook, line, sinker

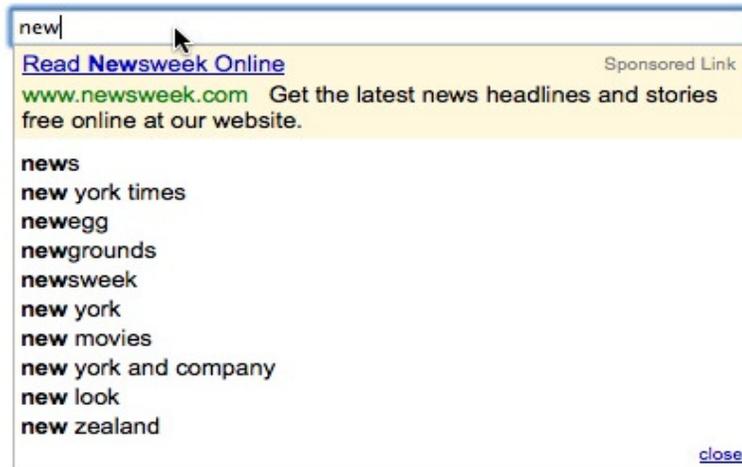
- User becomes the unwitting accomplice
- Opens email, clicks link or infected attachment
- Box is now popped and its on to the network



---

# Curiosity Not Only Kills the Cat...

---



## User psychology:

- *Google = Internet*
- *Google = Trust*
- *Internet = Trust*

- Malware authors use Search Engine Optimization to poison search results
- 2 month study finds Google serves 69% of total malware by search engine <sup>(1)</sup>
- 60% of top Google search terms delivered user to malicious sites in first 100 results <sup>(2)</sup>
- 10% of all malware analyzed by Cisco in Q3 2010 was encountered through the search engine <sup>(3)</sup>

<sup>(1)</sup> Barracuda Labs Report - July 2010

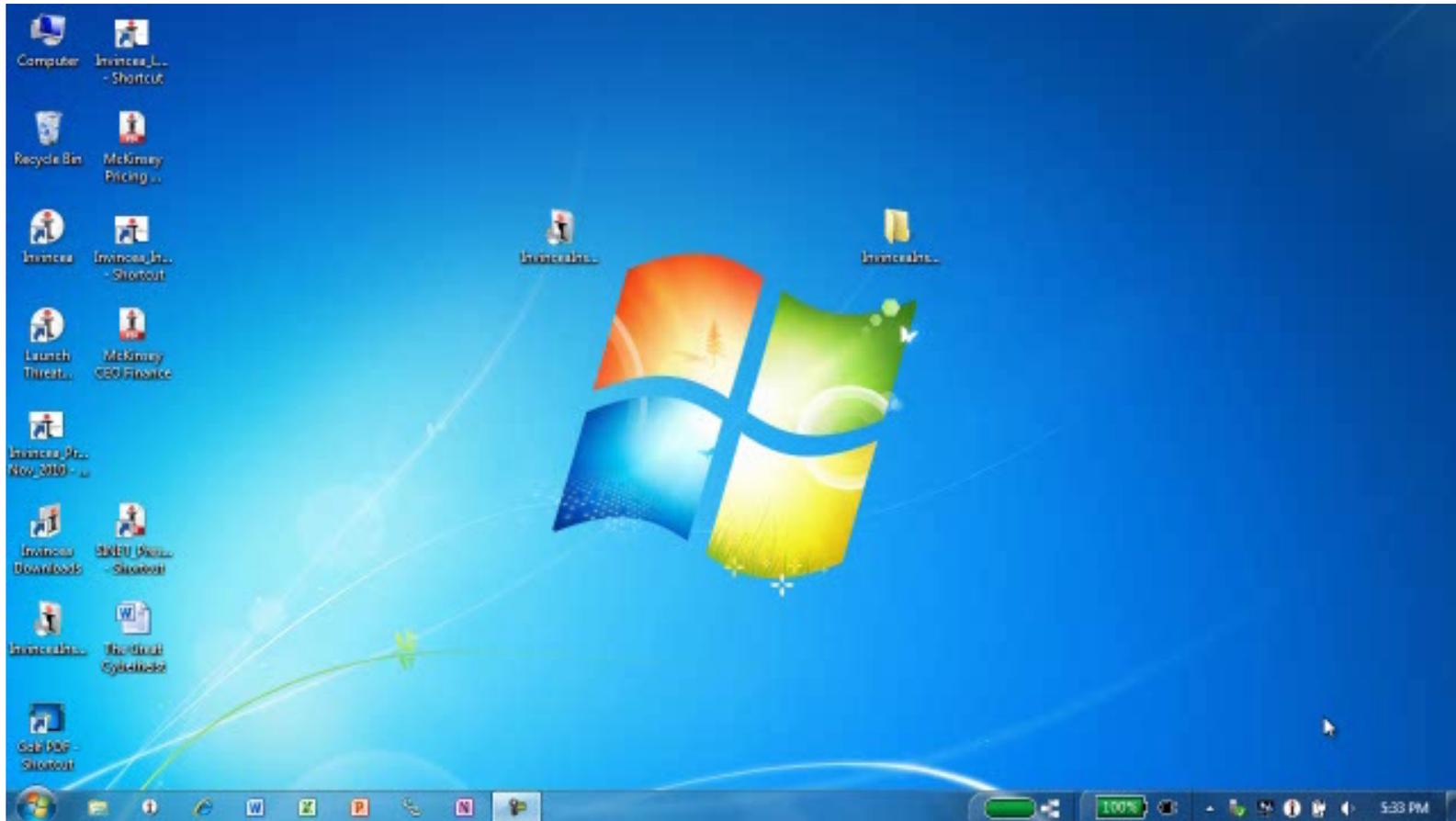
<sup>(2)</sup> McAfee threat report – November 2010

<sup>(3)</sup> Cisco threat report – November 2010

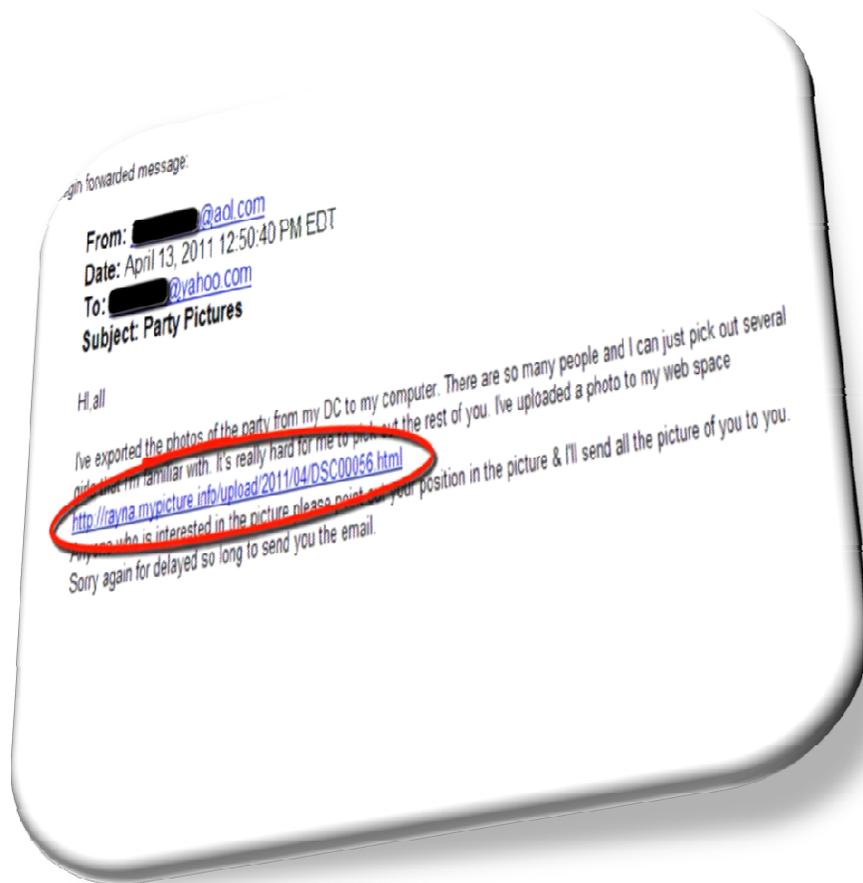
---

# *...it Gets Your Network Pwned!*

---



# How They Tried to Pwn Me...



- Targeted and well crafted inbound email sent to personal email account
  - Lowered security in home environment
  - Easy path for lateral movement
- Localized – referencing DC
- Socially engineered – spoofed to look like it came from a friend
  - Referenced birthday party over the summer
  - Referenced the name of one of my friends' daughters
- Similar to ORNL – directed to a drive by download site
- Very aggressive malware – designed to exfiltrate

---

# Case Study: Hacking a Security Company

## RSA – The Security Division of EMC

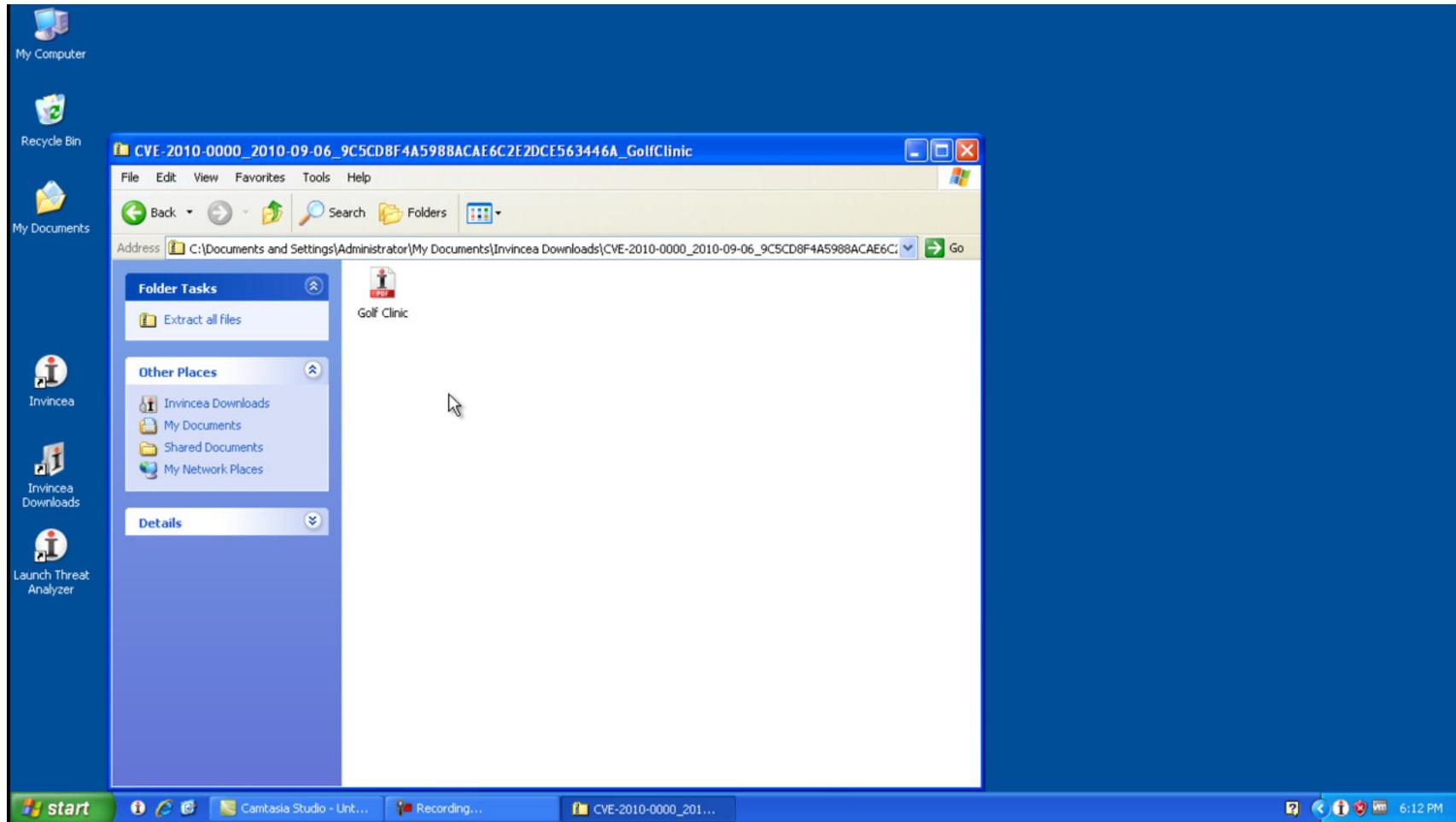
---



*Every organization has users...existing preventative solutions are failing us all.*

- Two different phishing emails sent to a small group of RSA employees
- Titled “2011 Recruitment Plan”
  - Stoke curiosity
- User actually retrieved from junk email
  - Use curiosity to kill the cat...i.e. pwn the network
- Attached document with zero-day Adobe Flash exploit
- Malicious link embedded in email
- Establish contact with C&C server
- Scope targets for lateral movement
- Get to the data and exfiltrate

# Demo: Getting Infected by Email Attachments



---

# Case Study: Hacking a National Lab

## Oak Ridge National Laboratories

---

April 21, 2011, 11:13AM

### Oak Ridge National Laboratory Cuts Off Internet, E-mail After Attack

by Christopher Brook



Share Recommend Cor

The Oak Ridge National Laboratory, a science and technology complex that houses one of the world's fastest computers, was forced to suspend Internet access and e-mail capabilities for employees on Friday in response to what has been described as a targeted phishing attack, according to Computerworld.

### Phishing Emerges As Major Corporate Security Threat

Added 21st Apr 2011

JAIKUMAR VIJAYAN, IDGNS

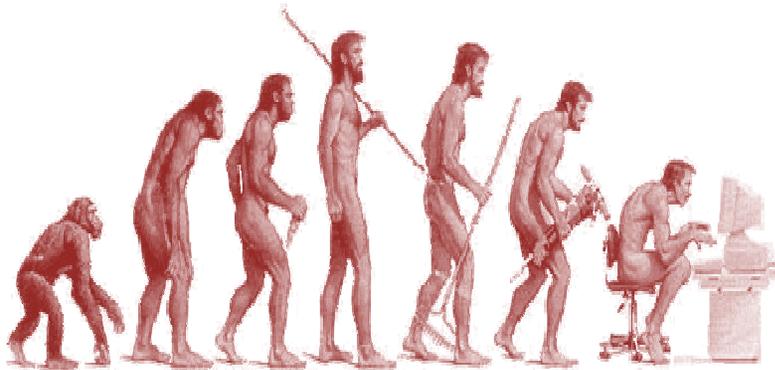
The successful use of phishing emails to breach secure organizations like [Oak Ridge National Laboratory](#) and RSA are stark reminders of the serious threat posed by what some experts have dismissed as a low-tech method of attack.

- 527 employees targeted
- 10% click through rate
- Email spoofed to come from HR
- Directed users to a website link for more information
- Drive by infection - click...click...boom!
- Caused the Lab to completely cut off Internet and external Email while remediating the breach

---

# Time for a Paradigm Shift

---



**Gartner.**

*“The Web is the primary source of malware infection.”*

**OGREN**  
group

*“A new approach to end-point security is needed.”*

 **IDC**  
*Analyze the Future*

*“The better approach is a protective layer that complements existing anti-virus solutions and that never allows those threats to enter the PC environment in the first place.”*

---

# Resilient Architectures

---



- Back to basic engineering
  - Put the glory back on those building secure systems
  - Engineer systems to be resilient to attack
- Develop architectures that separate untrusted code from trusted code bases
  - Treat EVERYTHING on or coming through the Internet as UNTRUSTED
- Some recent innovations behind sandboxing are a good step in the right direction...
- 100% virtualization – accept nothing less

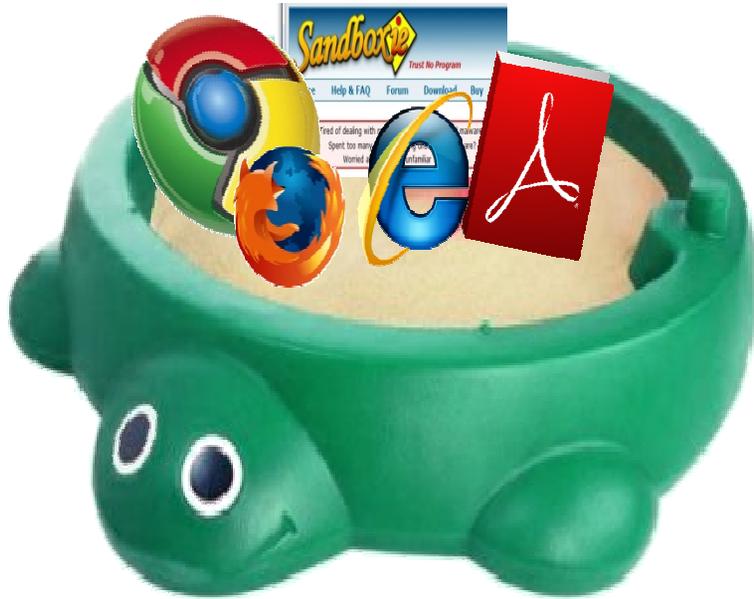
---

# Innovating for Today and Tomorrow...

## *Making Prevention Possible Once Again*

---

### 2010 “The Year of the Sandbox”

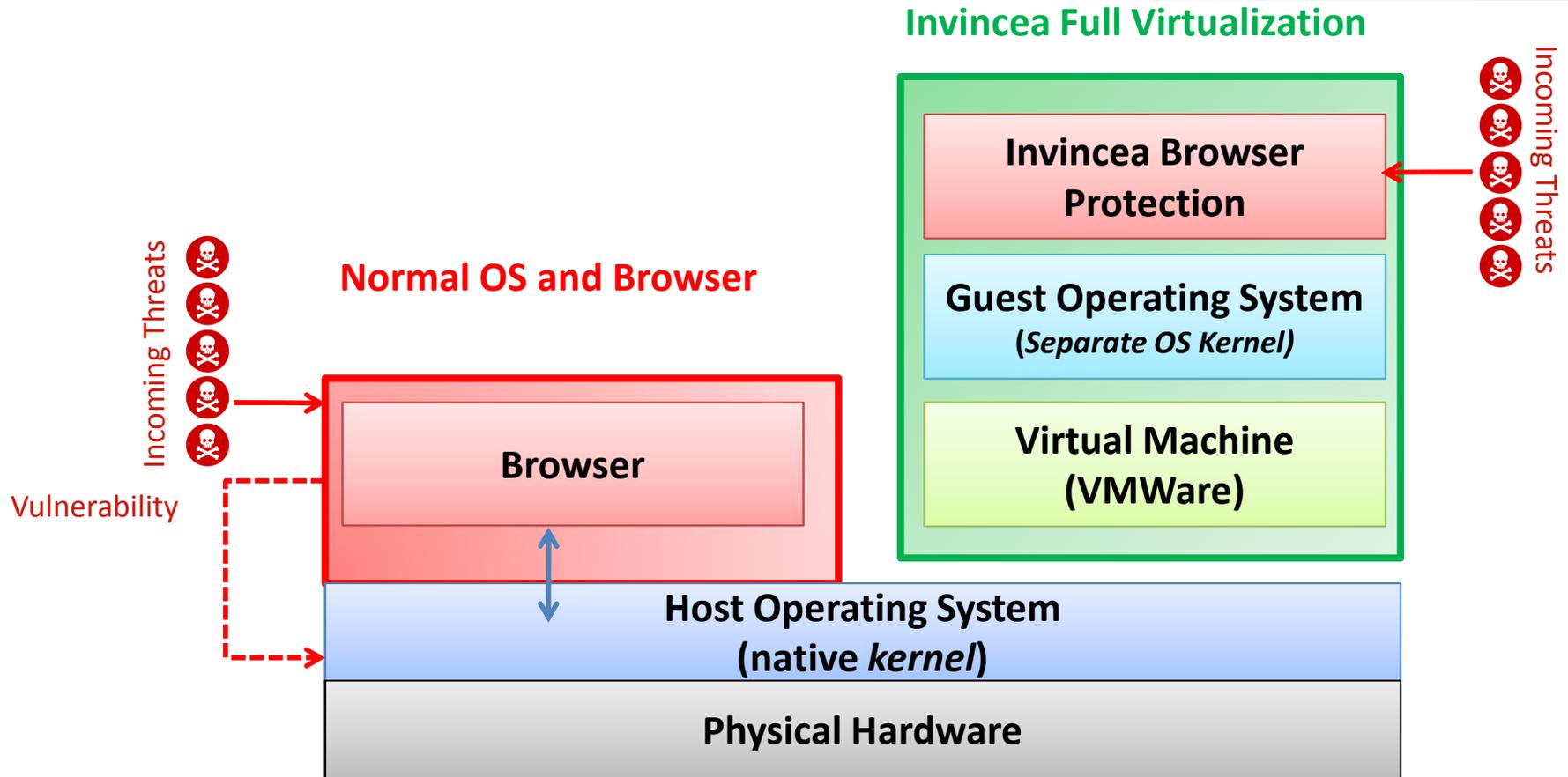


*Commendable efforts - but too much residual risk is left on the table...*

### 2011 “The Year we Turn the Tide”

- FULLY virtualized solutions developed under DARPA grant – commercially tested and available today
- Developed by security experts for the biggest security concerns
  1. Seamless segregation of browser and PDF reader from native operating system (STARTING point – vision is for all content types)
  2. Automatic, behavioral based detection and kill
  3. Forensic data capture and feed to larger infrastructure
  4. Restoration to pristine state
  5. Completely transparent to the user

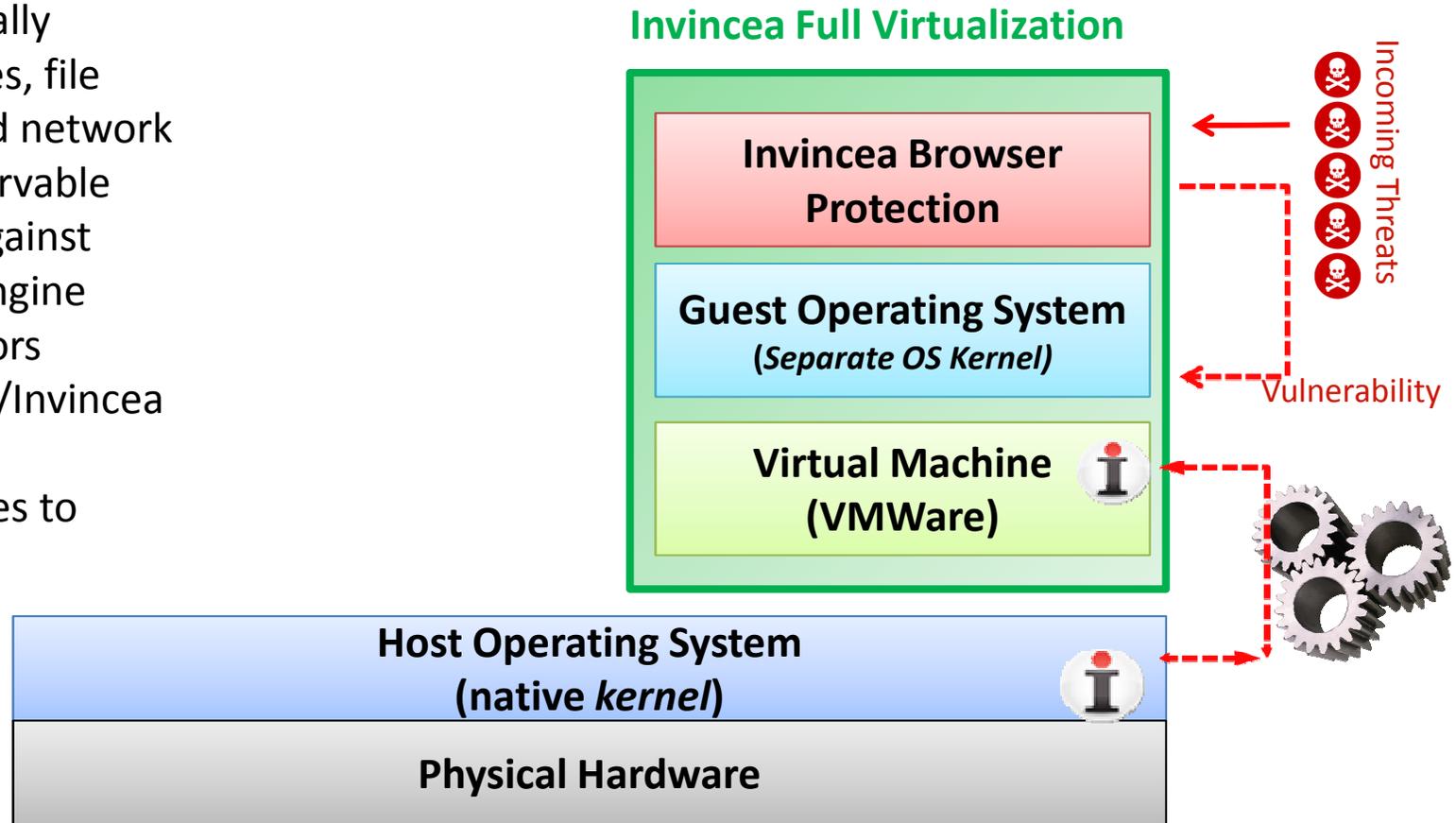
# Virtualization Protects the Desktop



- Compromise of Normal OS and Browser leads to direct compromise of Host OS
- Have to reimage entire system

# Virtualization Protects the Desktop

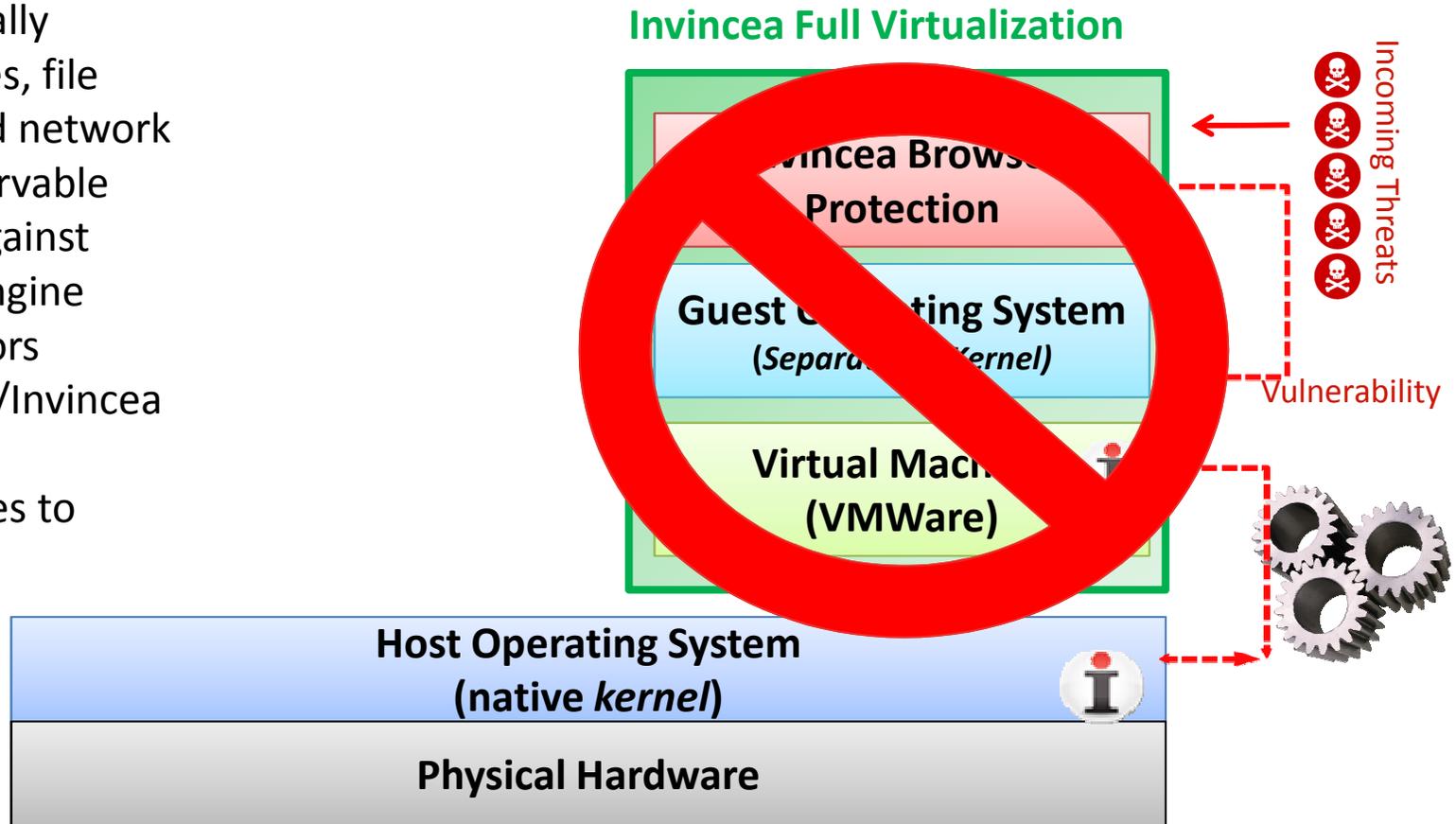
- 1) Invincea Internally monitors processes, file system, kernel and network
  - 2) Compares observable behavior of VM against allowable Rules Engine
  - 3) Invincea monitors externally the VM/Invincea comms
- Any unsafe changes to GuestOS/loss of communication Equals reset of VM



- Invincea (Guest Kernel) is distinct from host system
- Infections of the virtual browser and kernel do not effect Host OS

# Virtualization Protects the Desktop

- 1) Invincea Internally monitors processes, file system, kernel and network
  - 2) Compares observable behavior of VM against allowable Rules Engine
  - 3) Invincea monitors externally the VM/Invincea comms
- Any unsafe changes to GuestOS/loss of communication Equals reset of VM



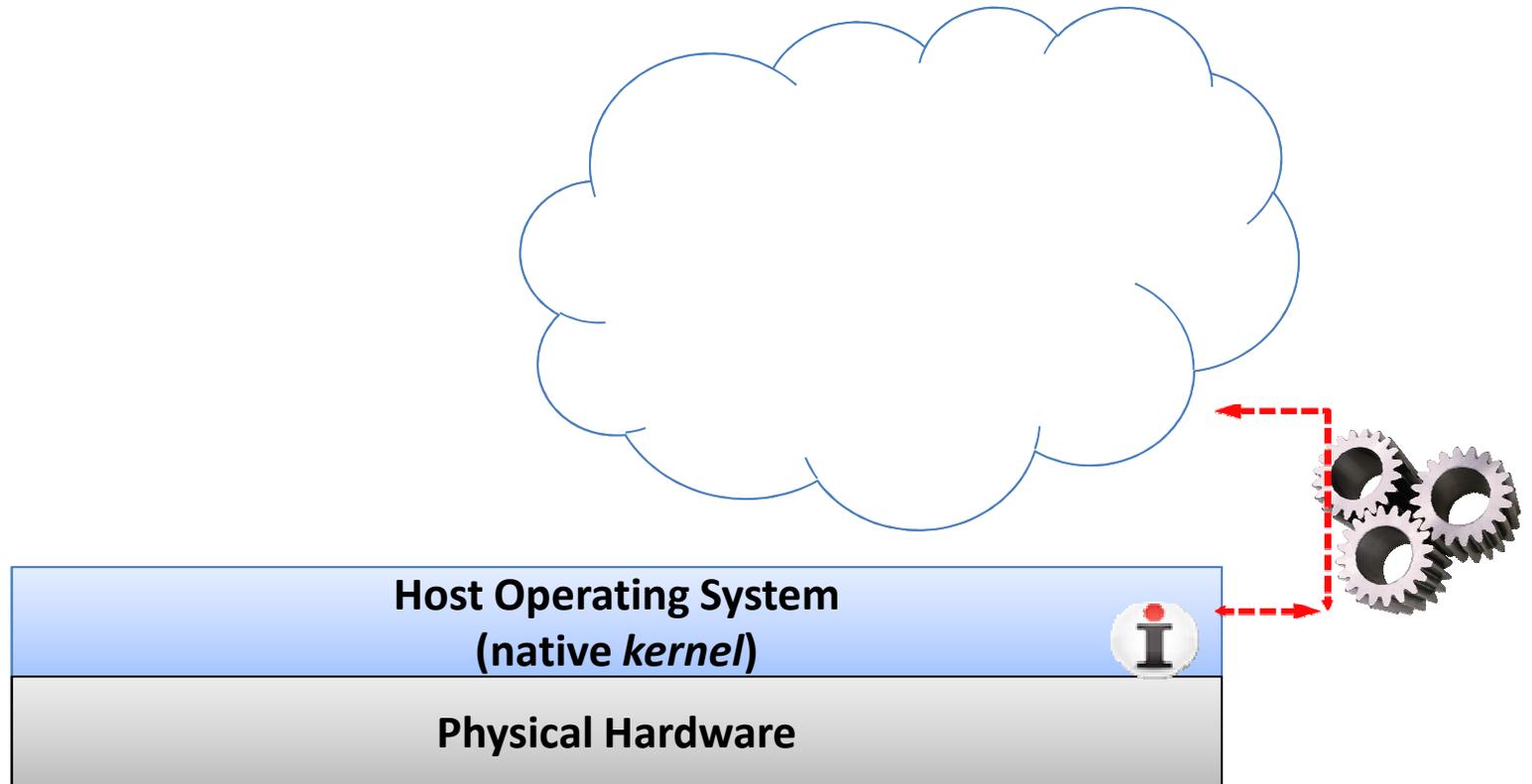
- Invincea (Guest Kernel) is distinct from host system
- Infections of the virtual browser and kernel do not effect Host OS

---

# Virtualization Protects the Desktop

---

4) VM is completely  
Removed



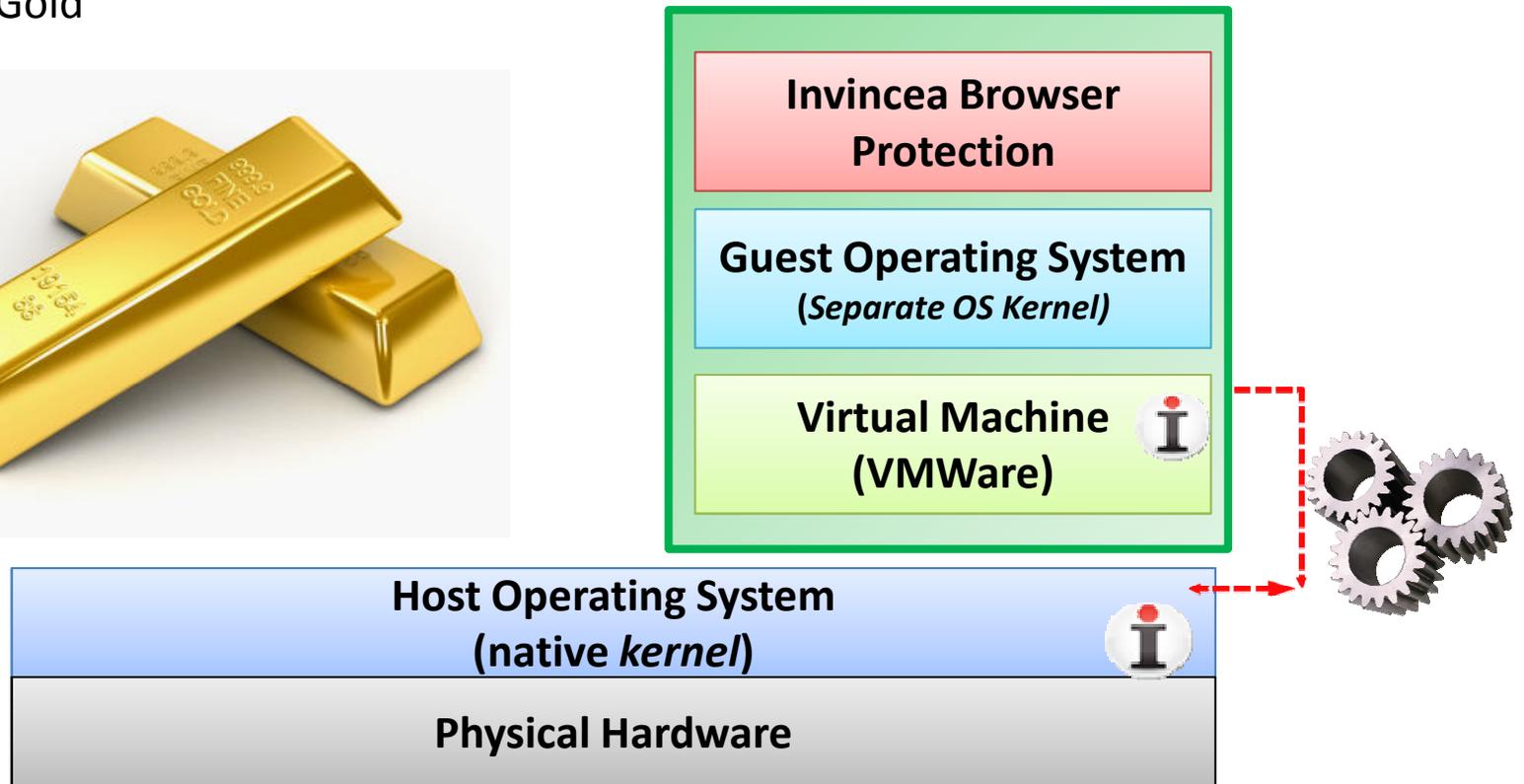
- Invincea (Guest Kernel) is distinct from host system
- Infections of the virtual browser and kernel do not effect Host OS

# Virtualization Protects the Desktop

5) VM snapshot back to pristine state off “Gold” image



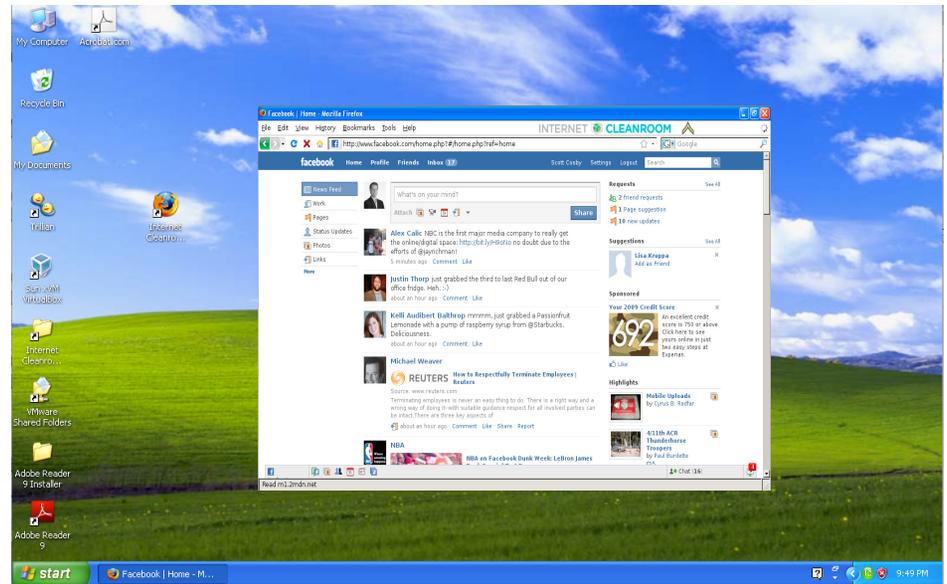
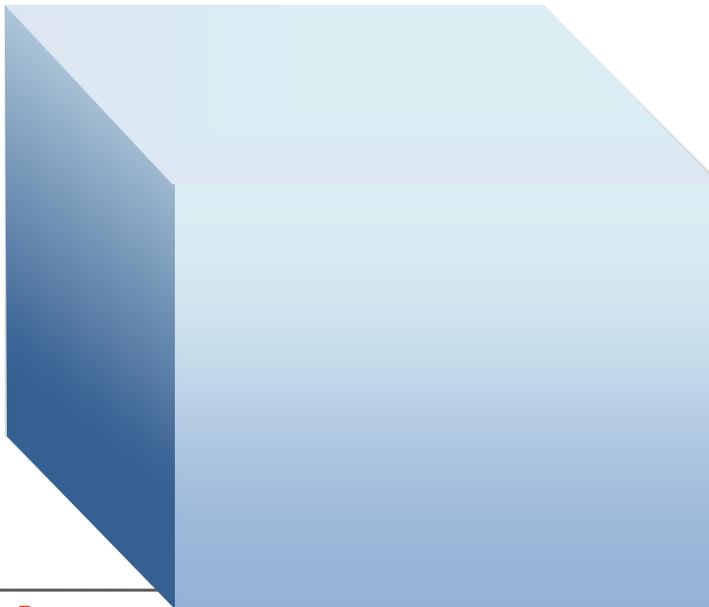
## Invincea Full Virtualization



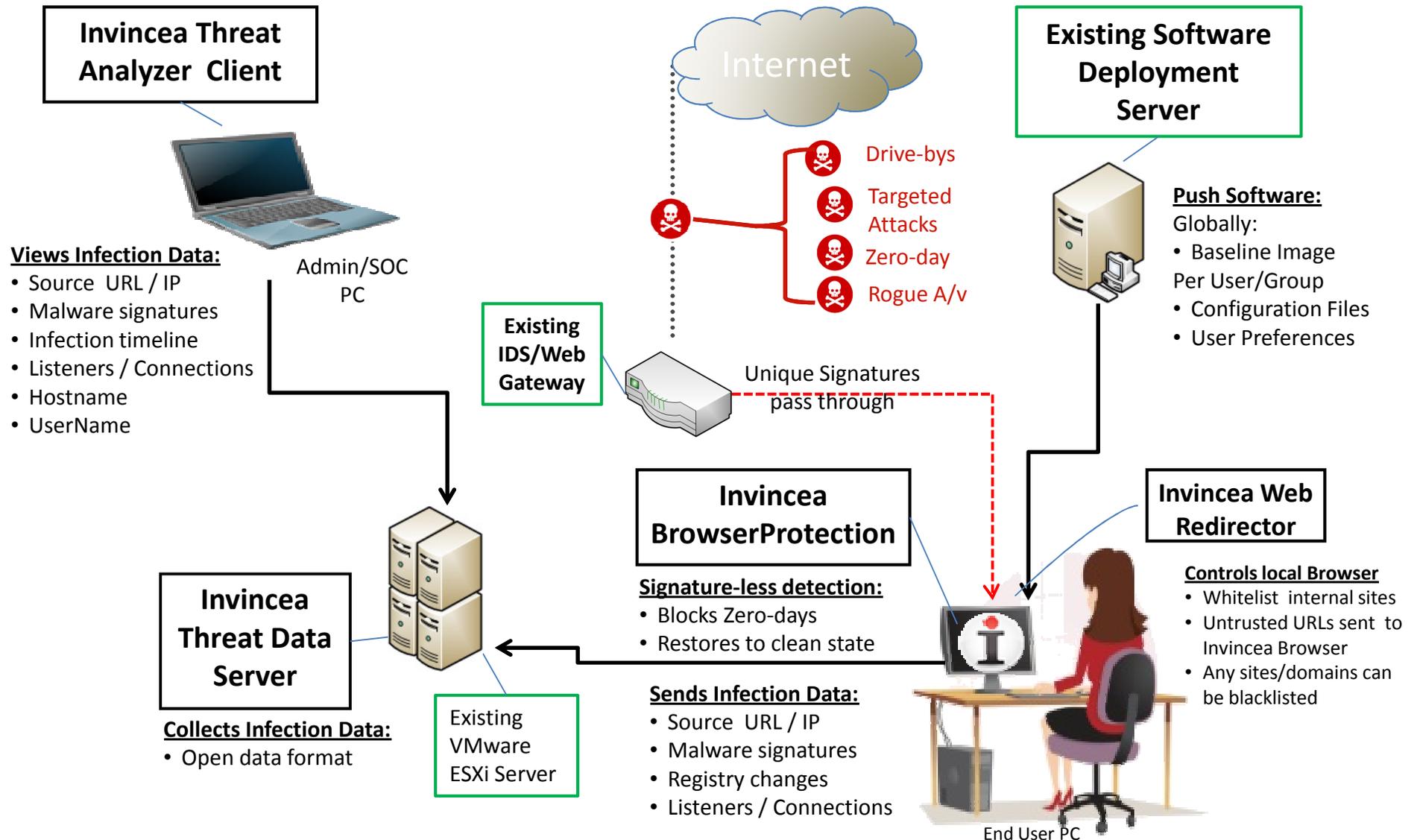
- Invincea (Guest Kernel) is distinct from host system
- Infections of the virtual browser and kernel do not effect Host OS

# Invincea Browser Protection

- Type II hardware virtualized browser environment
- Signature-free malware detection
- Generates real-time forensic threat intelligence
- Easy to use & deploy



# Invincea High-Level Architecture





---

# Changing the Game - The Invincea Model

---



Addressing the largest attack surface:

- ✓ Spear Phishing
- ✓ Drive bys
- ✓ Social Network Worms
- ✓ Poisoned SEO
- ✓ User Initiated Infections

- i** Drive **real-time situational awareness** by making **ALL** of your desktop browsers **malware detectors and forensics agents**
- i** **Protect the network from the user** and the user from himself...put him in a bubble while on the **Internet or interfacing with ANY untrusted content**
- i** Take Security decisions out of the user's hands
- i** Make the user's mistakes irrelevant to the security of your network
- i** Give the user free reign to complete his mission without fear for your overall security footing – zero trust with zero drag

# Recognition as a Game Changer

## SC Magazine “First Look”

*“Invincea effectively stops zero-day malware in its tracks.”*

*“Take a very close look at this. It is from a brand new company and I predict big things for it if the management team continues down the road they're on now.”*

***“What we didn't like: Nothing. This product does exactly what it claims to do and is completely transparent to the user.”***



The screenshot shows the SC Magazine website interface. At the top, there's a navigation bar with links like 'Home', 'News', 'Products', 'Blogs', 'Buyers Guide', 'Whitepapers', 'Jobs', 'Events', 'Subscribe', 'SC World Congress', and 'Archive'. Below this is a search bar and a topic center with categories like 'Financial Services', 'Health Care', 'Retail', 'Government', 'SC Awards', 'SC Canada', 'SC Scholars', and 'Cybercrime Corner'. The main content area features a prominent orange banner for 'SC eSymposium: Insiders with access | Jan. 25, 2011 | Click here for more Information'. Below the banner, there's a section titled 'FIRST LOOK Invincea browser protection' by Peter Stephenson, dated January 03, 2011. The article text begins with 'OK. So I wasn't all that impressed the first time I heard about this tool. It sounded like another "me, too" web browser product using the same, old, tired technologies that pretend to isolate malware. Yawn. Then I spent an hour with the product and the people at Invincea who came up with it and wow! Was I ever wrong at first blush. I really beat these guys up on the technology and methodologies they use, and they were like Teflon: Nothing stuck. So, before we even get started, here is my recommendation: Take a very close look at this. It is from...'. To the right of the article is a sidebar with social media sharing options (Print, Email, Reprint, Permissions, Font Size, Tweet, Like) and a 'MORE REVIEWS' section with a link to 'Strong authentication'. On the far right, there's a vertical banner for 'Applications Power Your Business' with social media icons for LinkedIn, YouTube, Facebook, and others.

- Winner – RSA 2011 Security Innovators Sandbox
- Winner – 2010 US East Coast Global Security Challenge
- Finalist – 2010 Global Security Challenge
- Finalist – 2010 SC Magazine Innovators Throwdown
- Finalist – SC Magazine 2010 Rookie Security Company of the Year

---

**Innovating to Combat the Malware Scourge**

---

**RSA<sup>®</sup>CONFERENCE 2011**

FEBRUARY 14-18 | MOSCONE CENTER | SAN FRANCISCO

***Invincea Named Most Innovative Company at RSA 2011***