7th Annual IT Security Automation Conference

Building Security Beneath the OS

Steve Orrin
Director of Security Solutions
Software and Services Group
Intel, Corp.

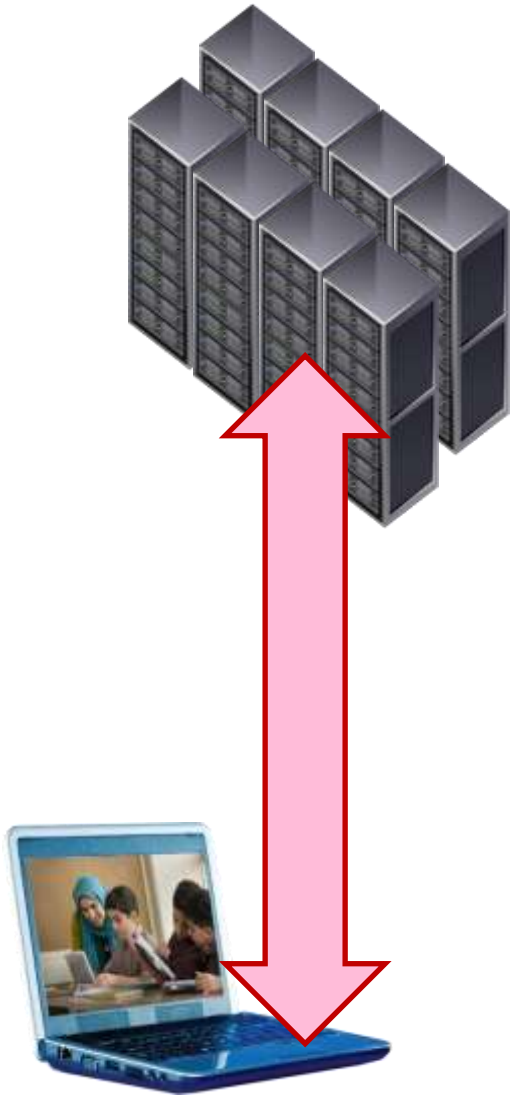
David O'Berry
Strategic Security Engineer
McAfee

Agenda

- Emerging Trend in Threats
  - Threats Targeting Servers in the Enterprise and Virtual Data Centers and the Cloud Threats
- The Need for HW Enabled trust
- Intel's TXT and How it works
- Using and leveraging HW rooted trust
- DeepSafe - Security Below the Operating System
-

Emerging Trend of Threats

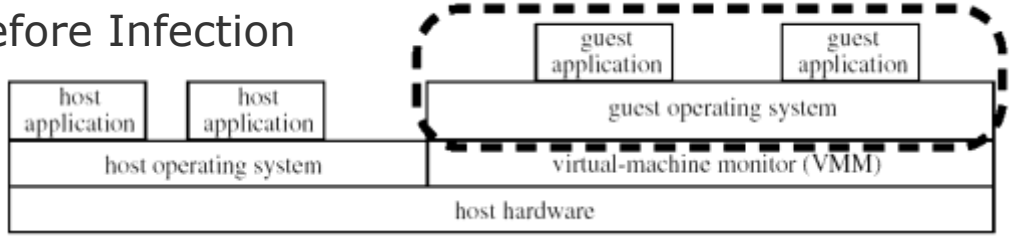
- Attacks, Malware and threats are targeting deeper in to the systems of clients
- They are also beginning to target or leverage the servers, data centers and the Cloud
- Thus the emerging need for hardware, firmware and under the OS software based protections and trust



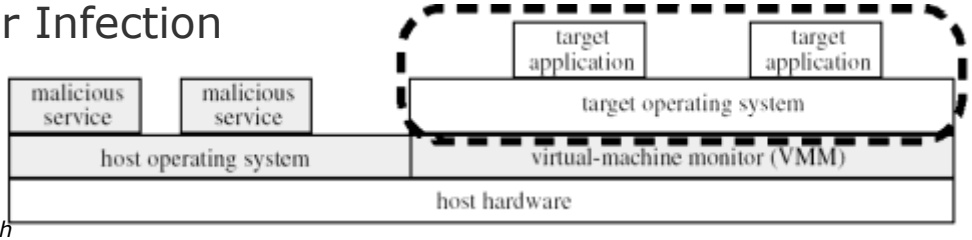
HyperJacking

- Hyperjacking involves installing a rogue hypervisor that can take complete control of a server. Regular security measures are ineffective because the OS will not even be aware that the machine has been compromised.
- Blue Pill/SubVirt use virtualization technology to create an ultra-thin hypervisor that takes complete control of the underlying operating system.

Before Infection



After Infection



SubVirt: Implementing malware with virtual machines
Samuel King & Peter Chen, University of Michigan
Yi-Min Wang, Chad Verbowski, Helen Wang, Jacob Lorch, Microsoft Research
BluePill
Joanna Rutkowska, Invisible Things

Clouds are Under Attack

- The Co-tenancy Problem
  - Researchers at the UCSD and MIT were able to pinpoint the physical server used by programs running on the EC2 cloud and then extract small amounts of data from these programs, by placing their own software there and launching a side-channel attack.
  - For more on the details of the attacks see: http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf
- VM Jumping/ Guest-hopping threats
  - Leverages vulnerabilities in Hypervisors that allow Malware to beat VM protections and gain access to other hosts. The driver for these attacks is that a Hypervisor has to provide at least the illusion of a "ring 0" for a guest operating system to run in.

Dark Reading on Virtualization Security
Thomas Ptacek
http://www.matasano.com/log/708/dark-reading-on-virtualization-security/

Need for Hardware based Trust

- New threats are emerging that are focused on attacking the pre-runtime environment
- Low-level attacks are hard to detect and can be difficult to recover from
- Emerging need for hardware-based trust

Introducing Blue Pill[1]

BIOS-level rootkit attack scary, but hard to pull off [2]

TTA #11: Hardware-Enabled Trust

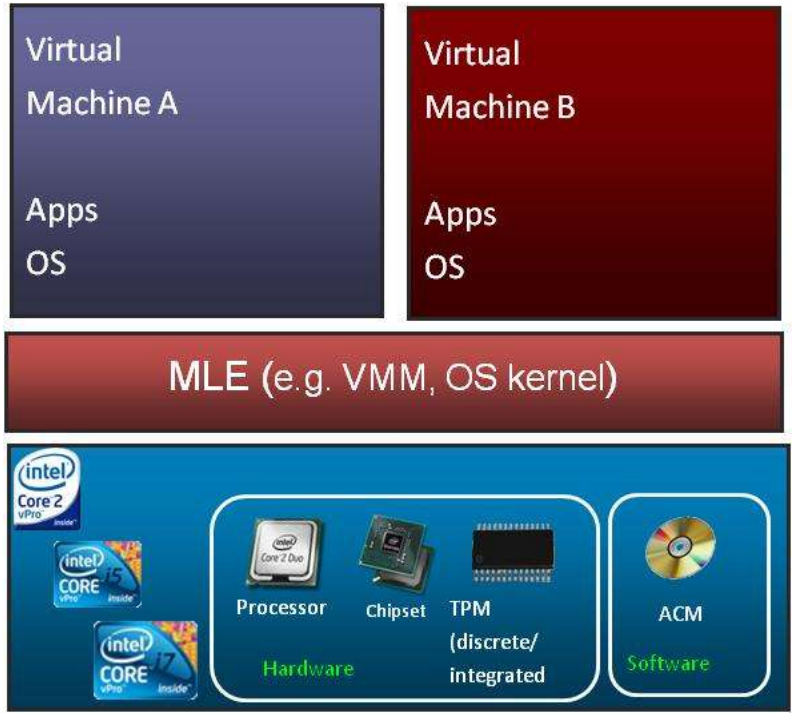
a. Hardware can be the final sanctuary and foundation of trust in the computing environment, based on the technologies that can be developed in the area of hardware-enabled trust and security. With cyber threats steadily increasing in sophistication, hardware can provide a game-changing foundation upon which to build tomorrow's cyber infrastructure. But today's hardware still provides limited support for security and capabilities that do exist are often not fully utilized by software. The hardware of the future also must exhibit greater resilience to function effectively under attack.

http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html
http://arstechnica.com/security/news/2009/03/researchers-demonstrate-bios-level-rootkit-attack.ars

Using Hardware Rooted Trust

A hardware based security foundation to build and maintain a *chain of trust*, to protect the platform from software based attacks

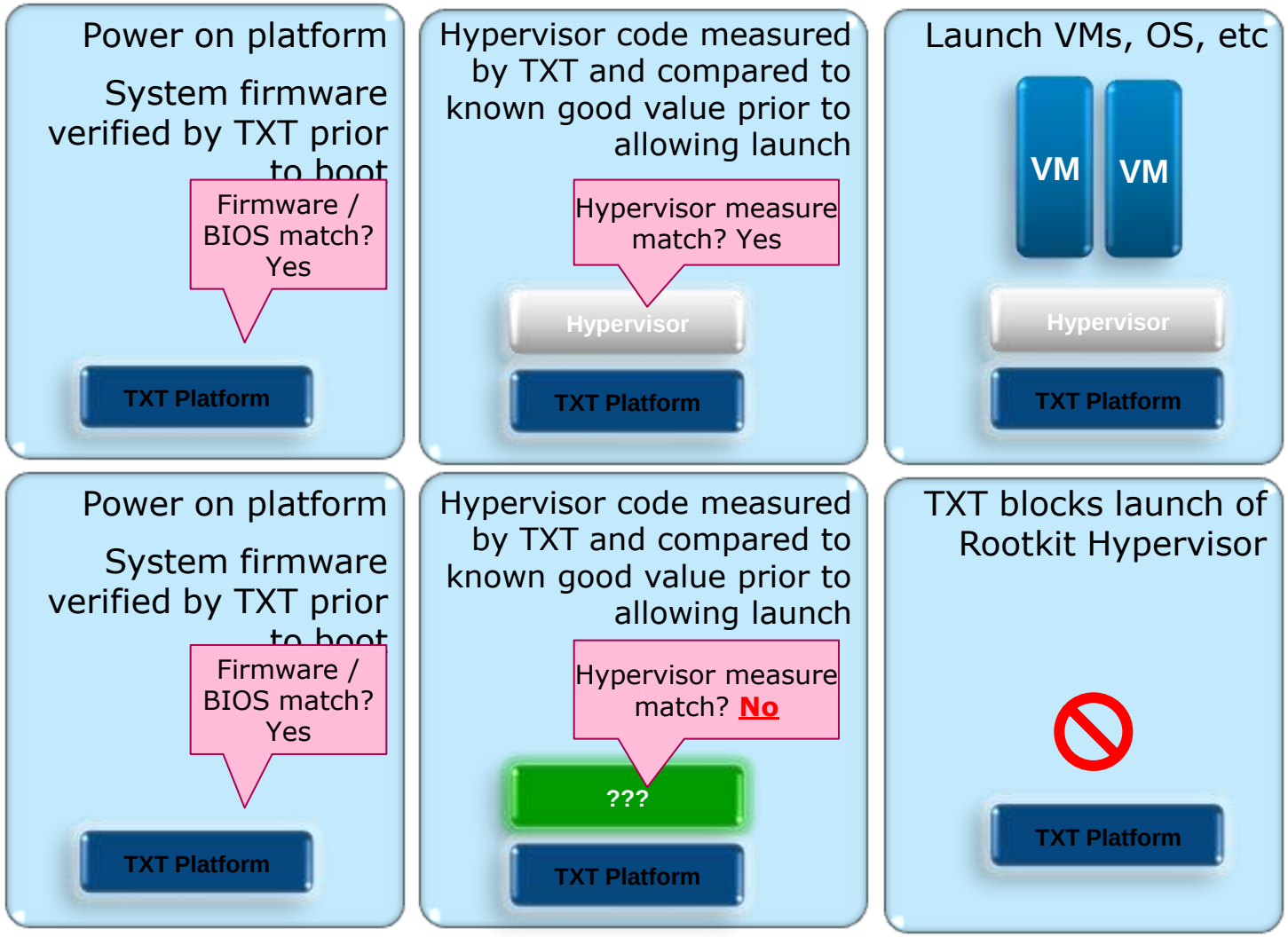
Example: Intel's Trusted Execution Technology (TXT) enforces control of the platform, measures launch components



- Trusted and verifiable systems
  - Implement policies/controls on top of a foundation of trust beginning in HW and up the stack
  - VMware, Parallels, Redhat and Citrix have products that support HW roots of trust and attestation

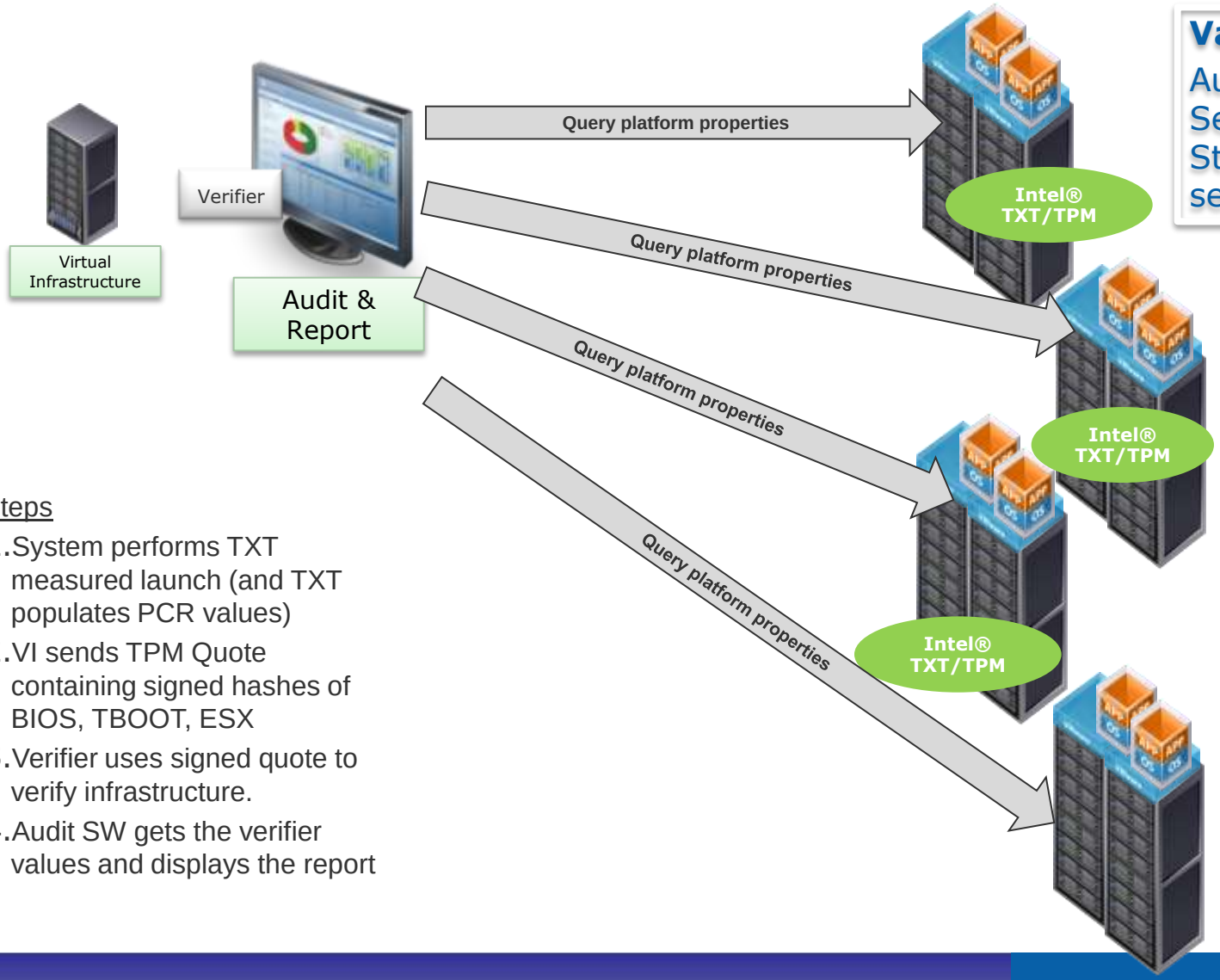
How it Works

Software can be measured and verified as known good



Unknown software is measured, detected and can be blocked

Platform Attestation and Audit

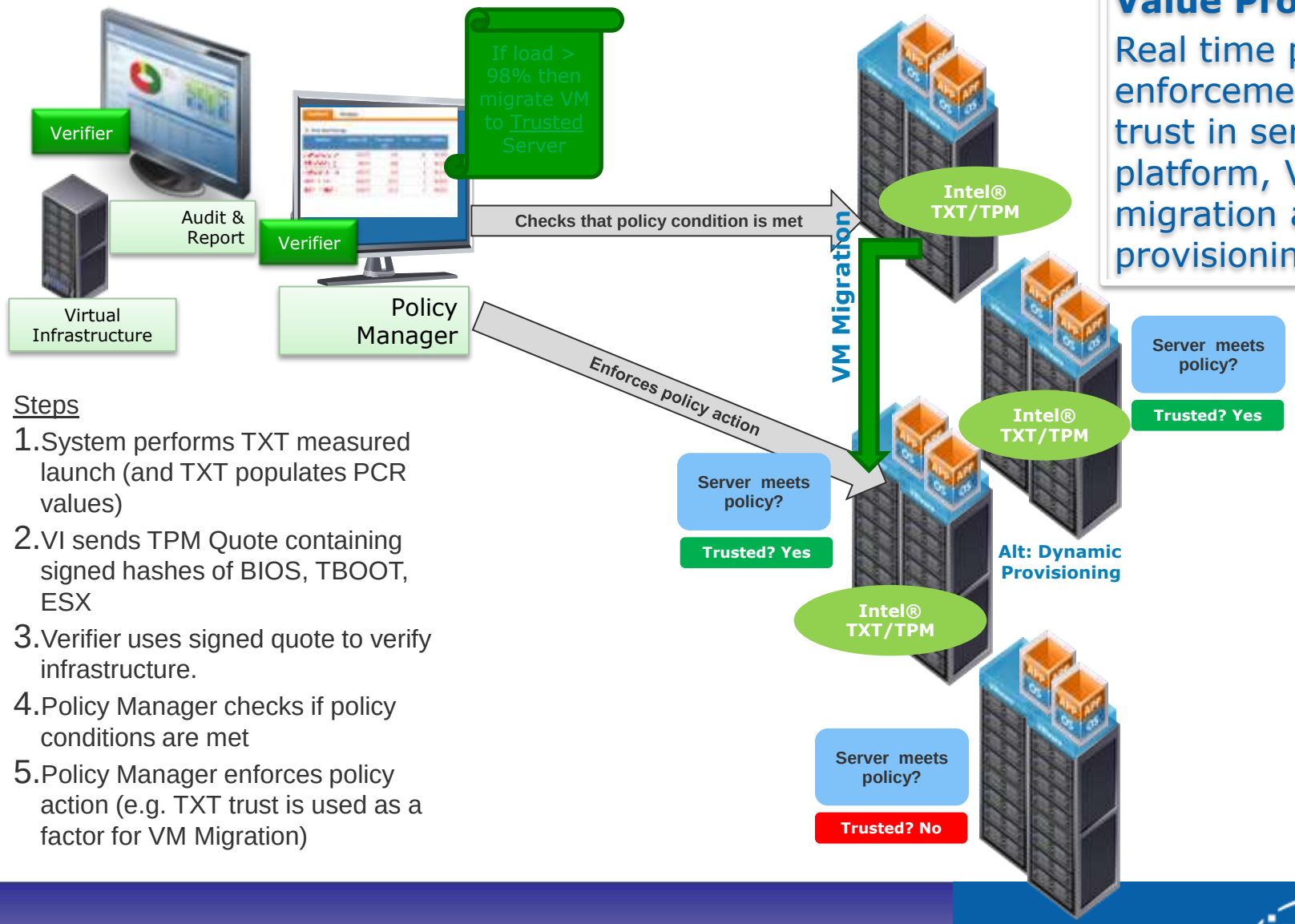


Value Proposition:
Audit of Trust of Server and Current Stack (workload, server, cluster)

Steps

1. System performs TXT measured launch (and TXT populates PCR values)
2. VI sends TPM Quote containing signed hashes of BIOS, TBOOT, ESX
3. Verifier uses signed quote to verify infrastructure.
4. Audit SW gets the verifier values and displays the report

Trusted VM Migration



Value Proposition:

Real time policy enforcement for trust in server platform, VM migration and provisioning

Steps

1. System performs TXT measured launch (and TXT populates PCR values)
2. VI sends TPM Quote containing signed hashes of BIOS, TBOOT, ESX
3. Verifier uses signed quote to verify infrastructure.
4. Policy Manager checks if policy conditions are met
5. Policy Manager enforces policy action (e.g. TXT trust is used as a factor for VM Migration)

Using Trusted Compute Pools

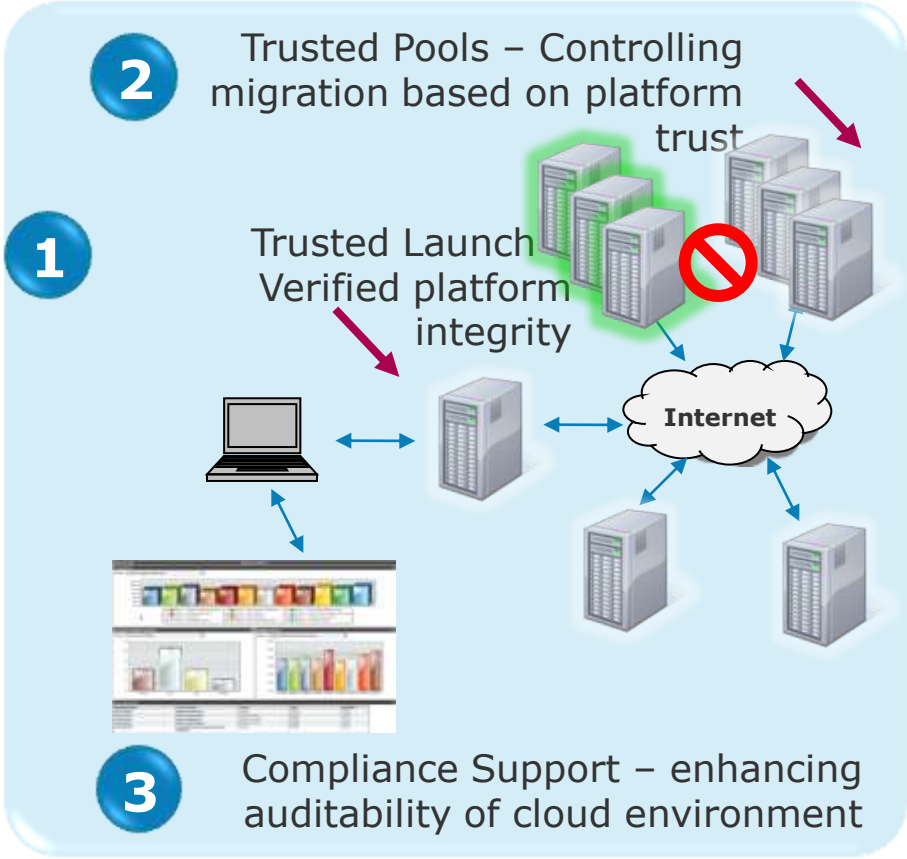
Addresses critical needs in virtualized & cloud use models

- Provides control to ensure only trustable hypervisor is run on platform
- Protecting server prior to virtualization software boot
- Launch-time protections that complement run-time malware protections– A/V, intrusion detection, etc
- Compliance Support

Control VMs based on platform trust

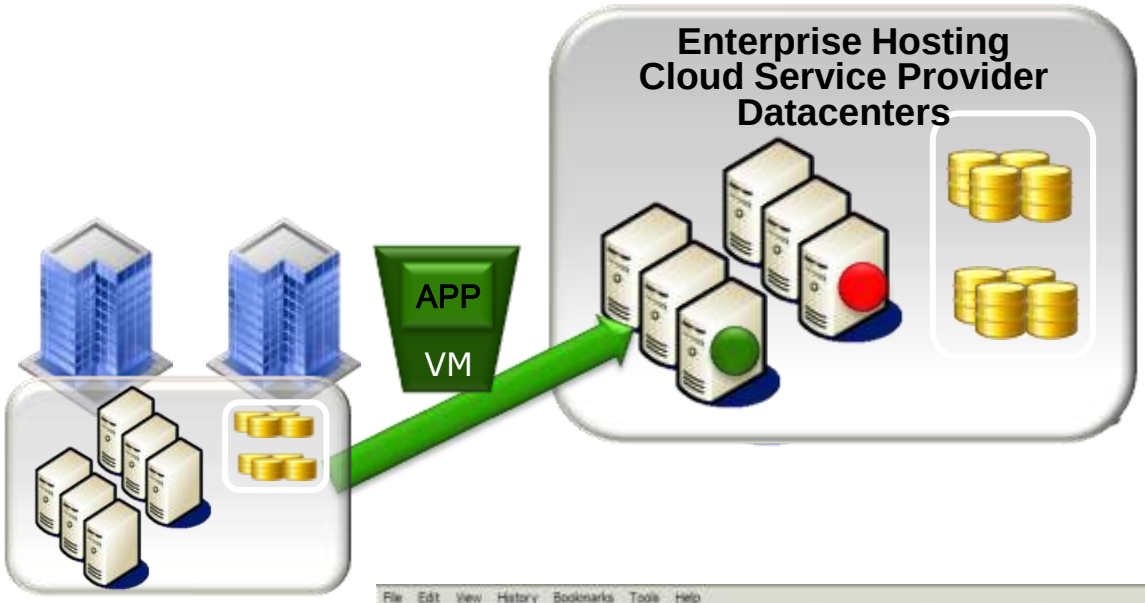
- Pools of platforms with trusted hypervisor
- VM Migration controlled across resource pools
- Similar to clearing airport checkpoint and then moving freely between gates

Work with your Service Providers & CSPs to require better controls and monitoring on your workloads/data

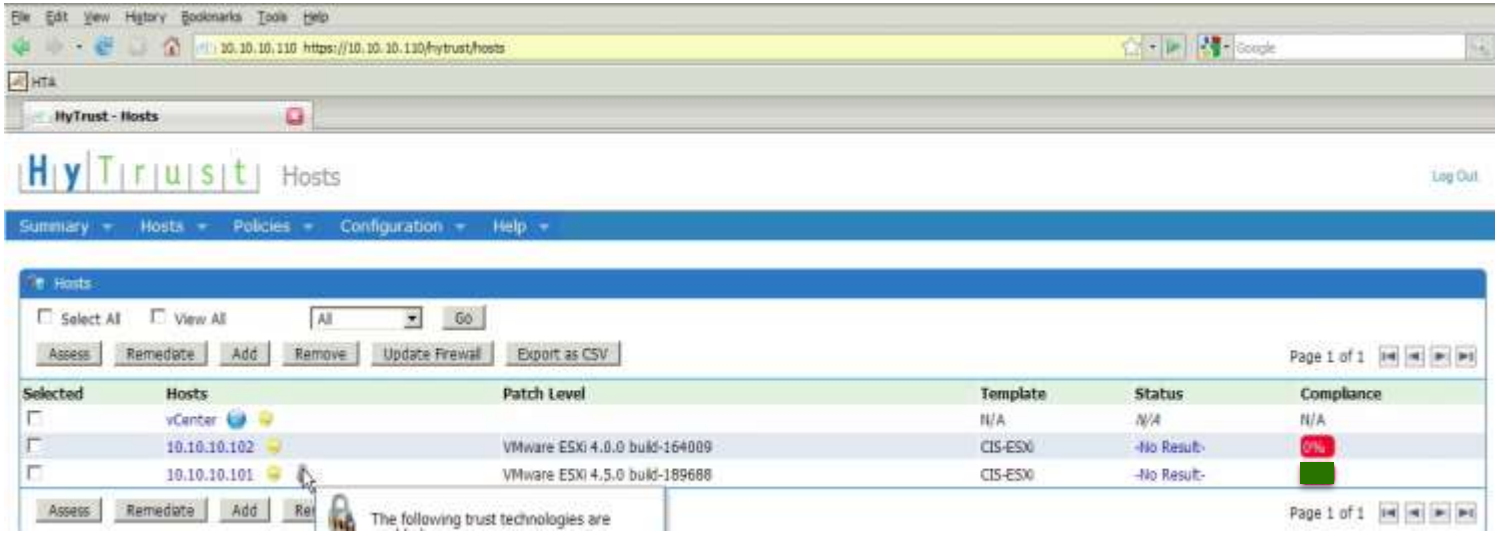


http://software.intel.com/en-us/articles/intel-cloud-builders-reference-architecture-library/#enhance_security

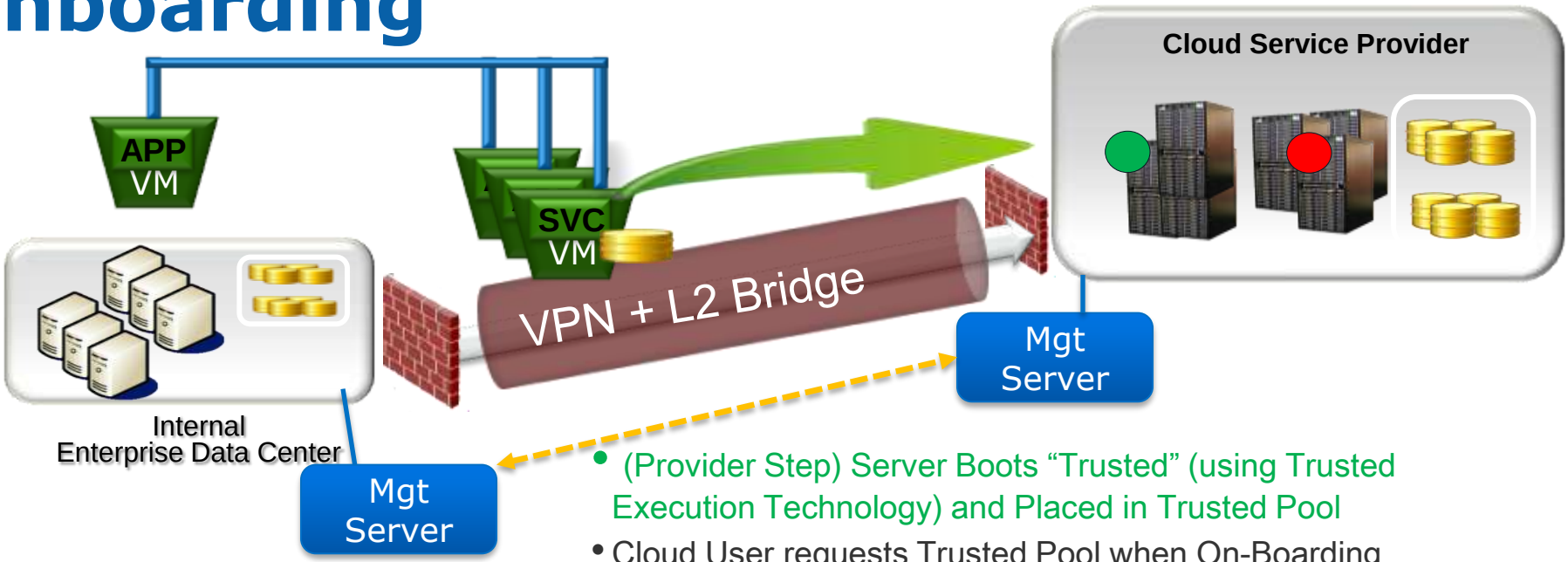
Example: Trusted Compute Pools



- Hypervisor Boots in Trusted Manner (using Intel Trusted Execution Technology)
- Trusted Server Placed in Trusted Pool
- Cloud User specifies Trusted Pool when On-Boarding Application



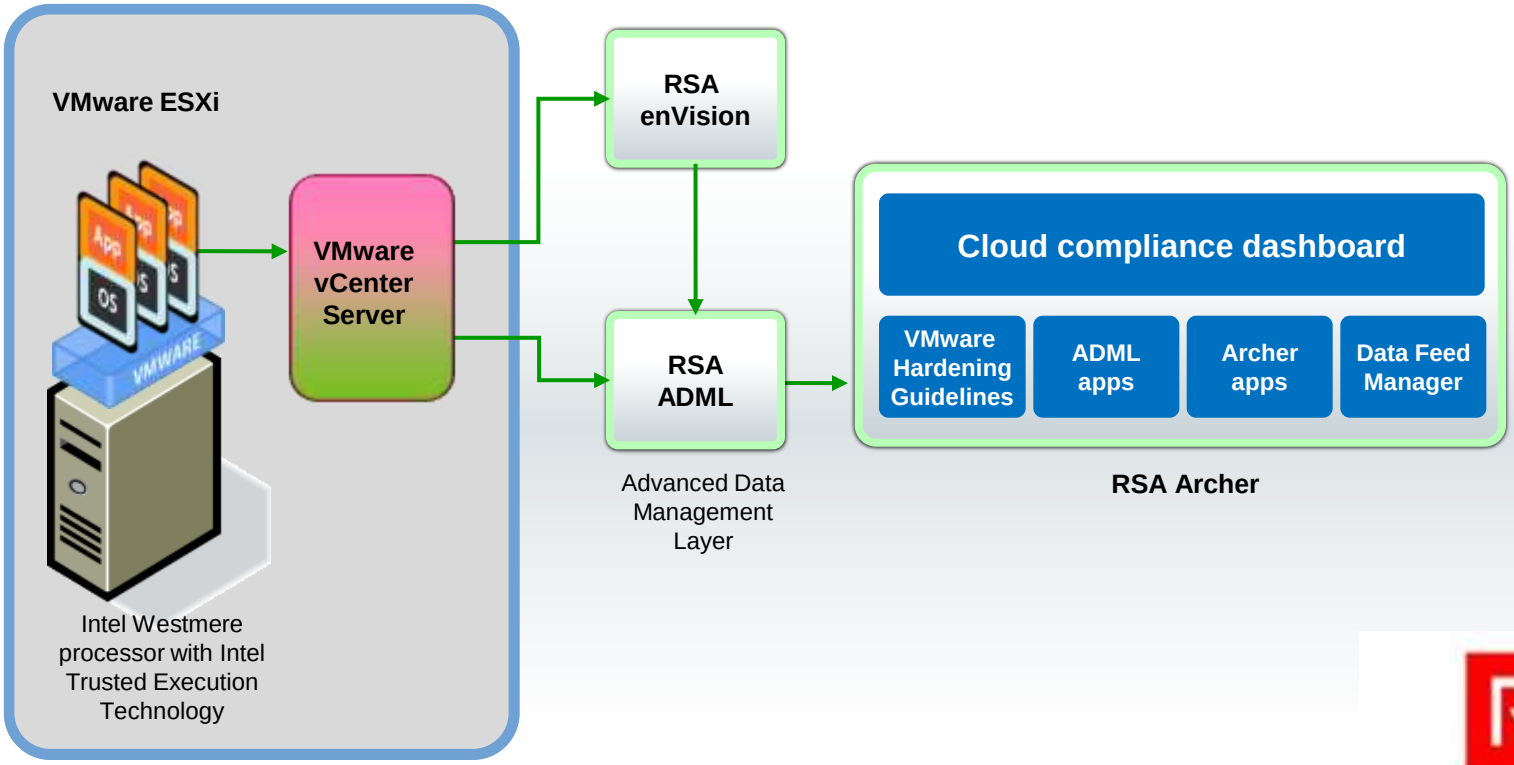
Cloud Subscriber: Secure Cloud Onboarding



- (Provider Step) Server Boots "Trusted" (using Trusted Execution Technology) and Placed in Trusted Pool
- Cloud User requests Trusted Pool when On-Boarding Application
- Virtual Machine placed in Trusted Pool
- Migrations & Location Compliance etc. managed by Policy

Example:
Cloud Compliance Architecture

Measuring and Monitoring Cloud Infrastructure Security



RSA
The Security Division of EMC

Deep Safe

Security Below the Operating System

David O'Berry
Strategic Systems Engineer

October 31, 2011

- David O'Berry, Previously Director of Strategic Development and ITS for SC Probation, Parole, & Pardon Services
  - During my 19+ years with South Carolina
  - MS-ISAC Executive Board
  - SC Security Domain Chairman and Collaboration TL
  - Trusted Computing Group's Customer Advisory Council (TNC-CAC)
  - Chairman, TOG's "Improving The Digital EcoSytem Workgroup"
  - Chapters Published on IF-MAP, SCAP, TNC and Standard's Based Defense/Mitigation (ISMH 09,10,11)

- My Previous Life's Work and the IT Environment?
  - 800+ users, rapidly growing ext. user-base (1000s)
  - 100% Mobile capable – Plan started in 2002
  - 26 Full-time IT including development , engineering, help desk, & remote support
  - 53 remote sites, decentralized work force

- Heterogeneous Deployment including Open Standards, Open APIs, and Open Source:
  - Core: McAfee, Dell, Juniper, APC
  - Network: Juniper, BlueCoat, Citrix, Imprivata
  - Data: McAfee EEPC, Device Control, Host DLP
  - Endpoint: McAfee AV, HIPS, Policy Auditor
  - Management: McAfee's ePolicy Platform, STRM, NSM Manager, Cacti & other "Open Source" products

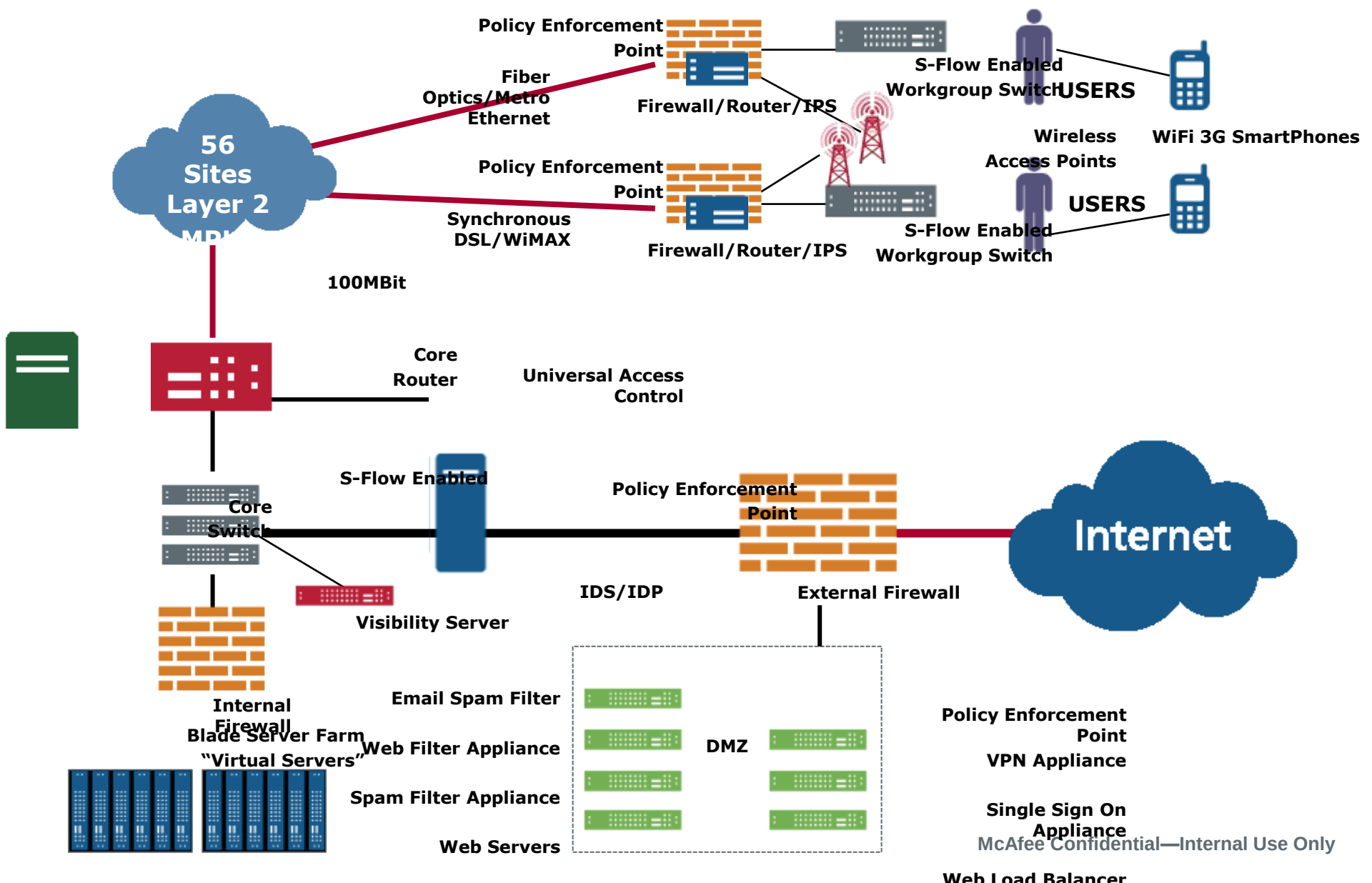
DeepSAFE – Why?

- Cyber criminals continue to develop advanced, stealth techniques used by malware to evade and subvert current security solutions running within the operating system.
- Something had to change and with that in mind Intel and McAfee decided to embark on a new generation of security products, enabled by existing chip technology with protection located below the operating system, designed to expose and stop advanced stealth attacks. DeepSAFE prevents what existing security solutions often cannot even detect.

Same Problems – New Day?

- Current security solutions provide protection within the OS
- Cyber criminals are circumventing this protection with advanced stealthy threats
- Current security solutions are ineffective at preventing these threats

Network Design: "No More Borders"



Challenges Compound

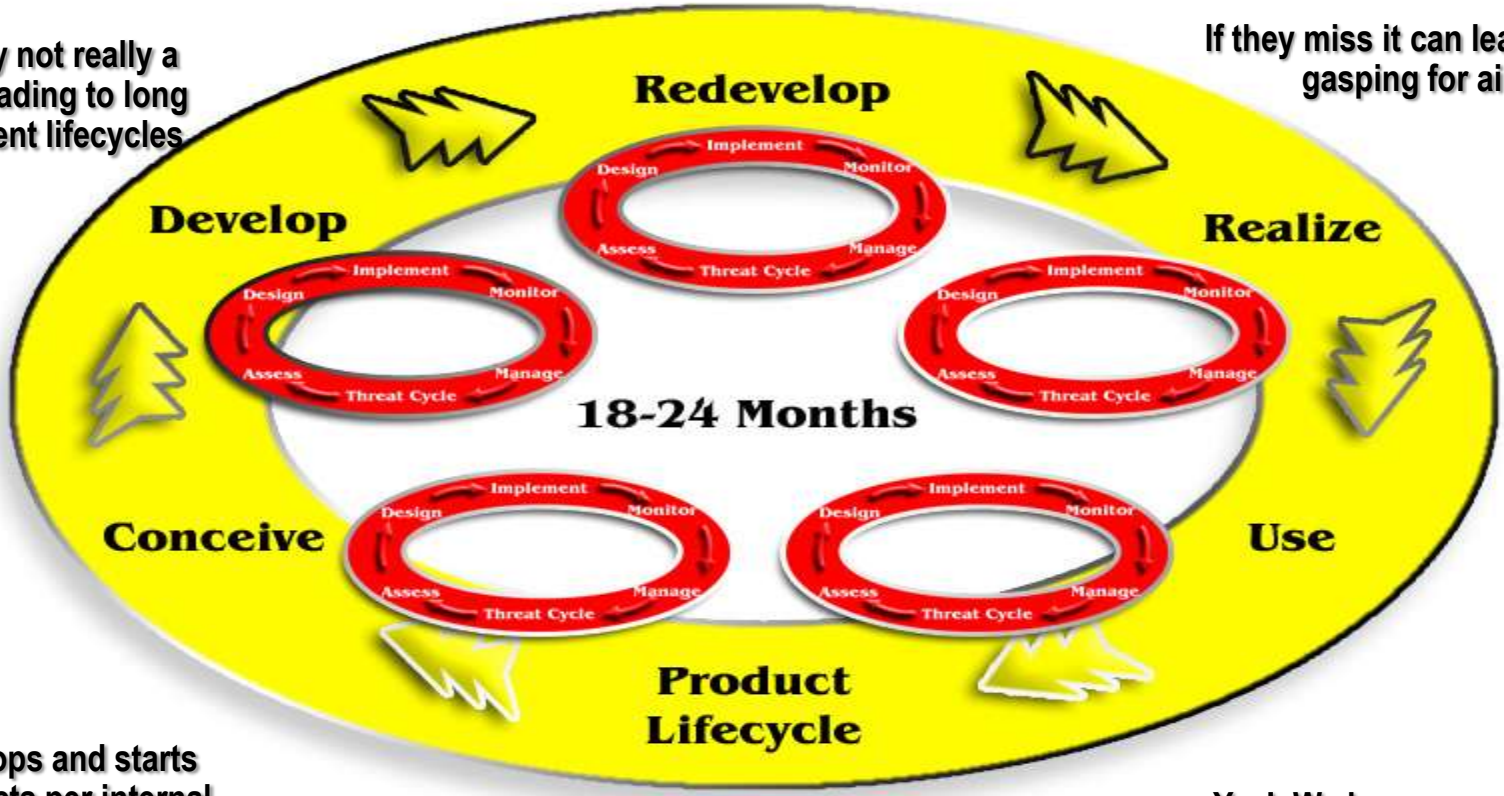
- Ubiquitous access from a steadily multiplying number of devices
- A user community that needs to be saved from itself but does not realize that fact and struggles against security and “control” at every turn
- Vendors that follow old school product marketing cycle irrespective of customer needs and what risks were based on rapidly evolving new threat lifecycles
- Rapidly evolving threats both in number and complexity
- Revolutionary new tools to deliver these threats

Product Cycle vs. Threat Cycle : We MUST Get Ahead of the Curve!

McAfee
An Intel Company

Modularity not really a concern leading to long development lifecycles

If they miss it can leave you gasping for air



Vendor stops and starts with products per internal challenges and market changes

Yay! We have a product to counter a threat that changed to something that requires a new product…wait?

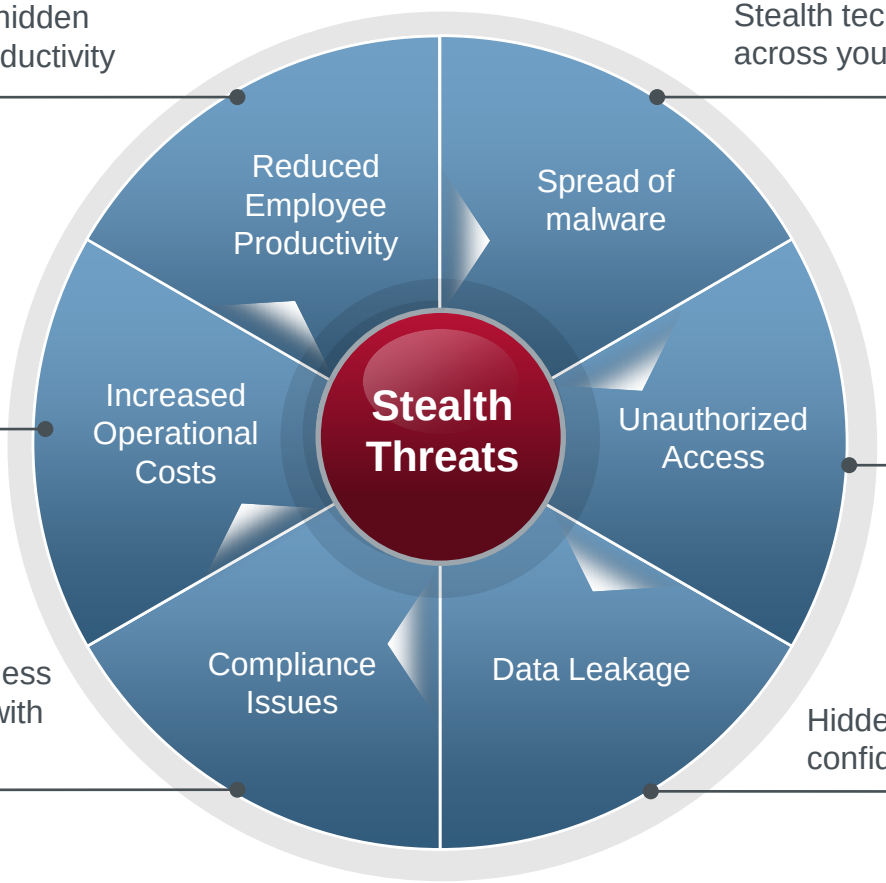
Stealth Attacks Will Continue

- 110,000 new rootkits detected each quarter
- More than 1.8 M unique rootkits
- More malware using rootkits to evade detection
  - TDSS rootkit is used as a persistent backdoor to install other types
  - Stuxnet and Son of Stuxnet
  - SpyEye is hidden with a rootkit to steal banking credentials

Stealth Techniques Increases Risk Exposure

Slow system performance from hidden threats decreases employee productivity

Stealth techniques to spread malware across your enterprise i.e. Zeus



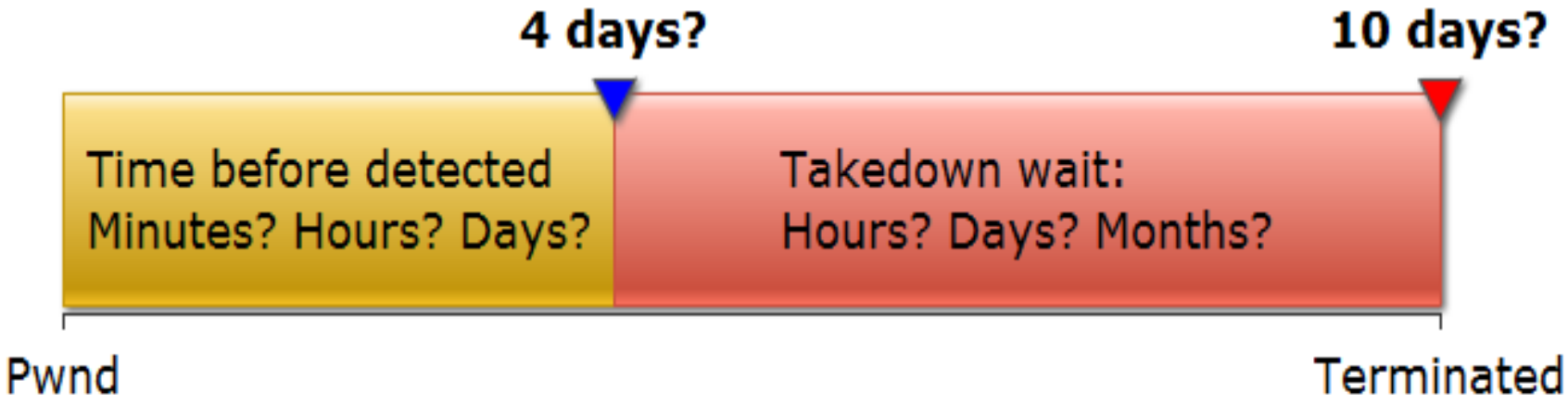
"Re-imaging" endpoints to remove hidden malware infections

Koobface threat used stealth techniques to secretly turn an endpoint into a BOT

Stealth malware puts your business at risk being out of compliance with privacy regulations and policy

Hidden key loggers quietly steal confidential and personal information

FIXME: (please)



Free Resources for Bot Master

Courtesy of maawg.org

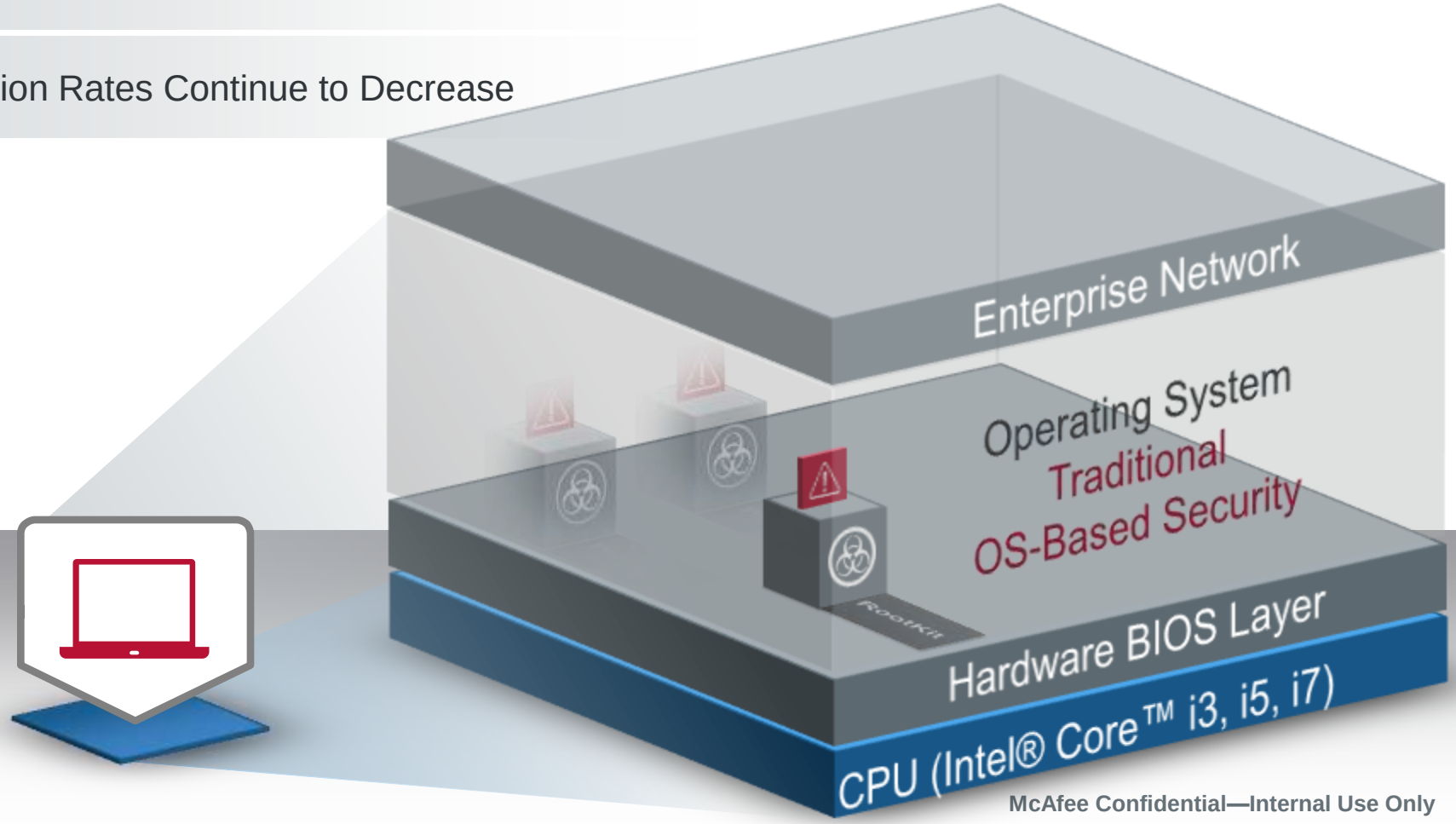
a few thousand C&Cs...

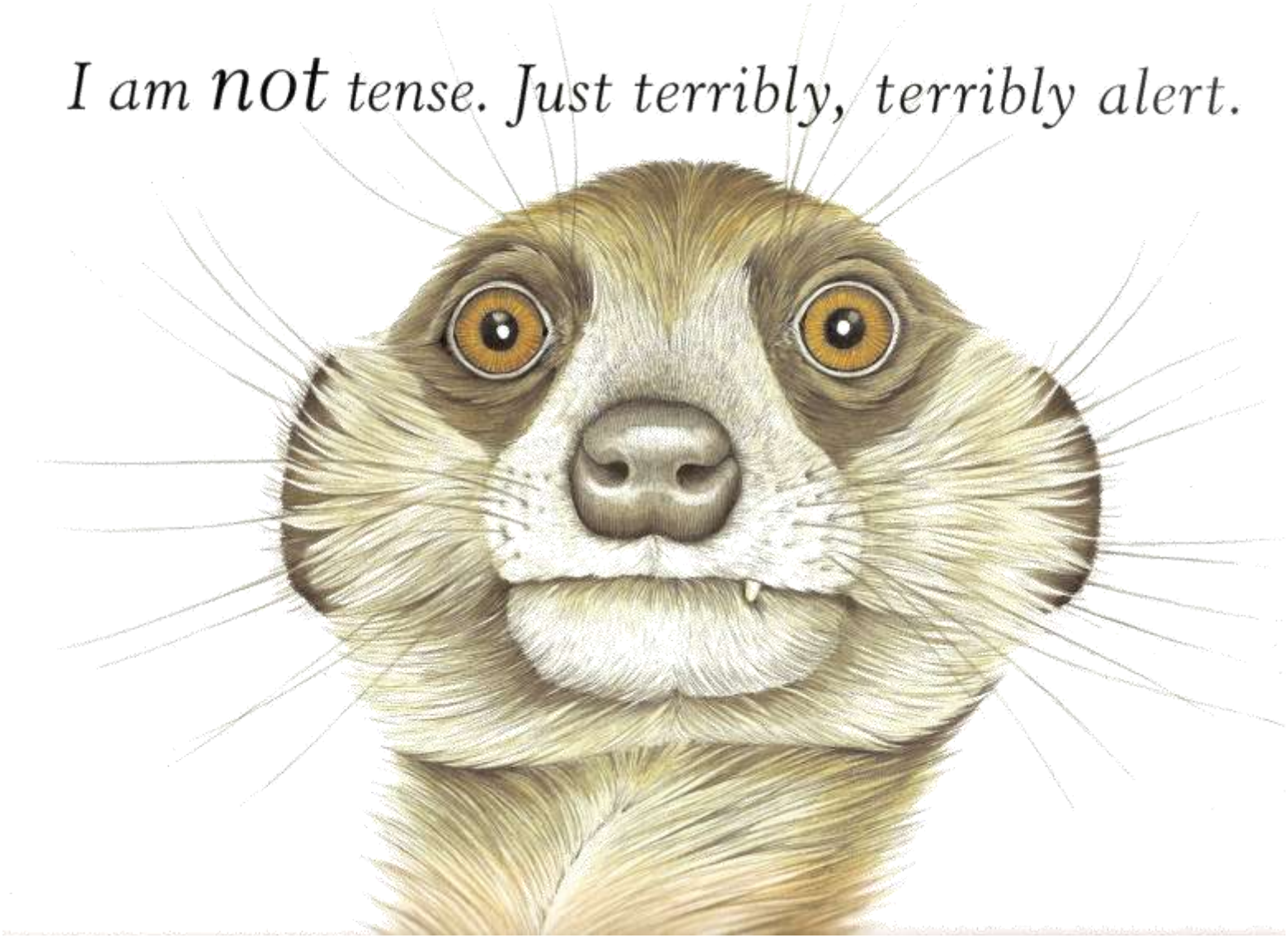
tens of millions of infected drones

Traditional Security: No Match for Current Attack Vectors

McAfee An Intel Company

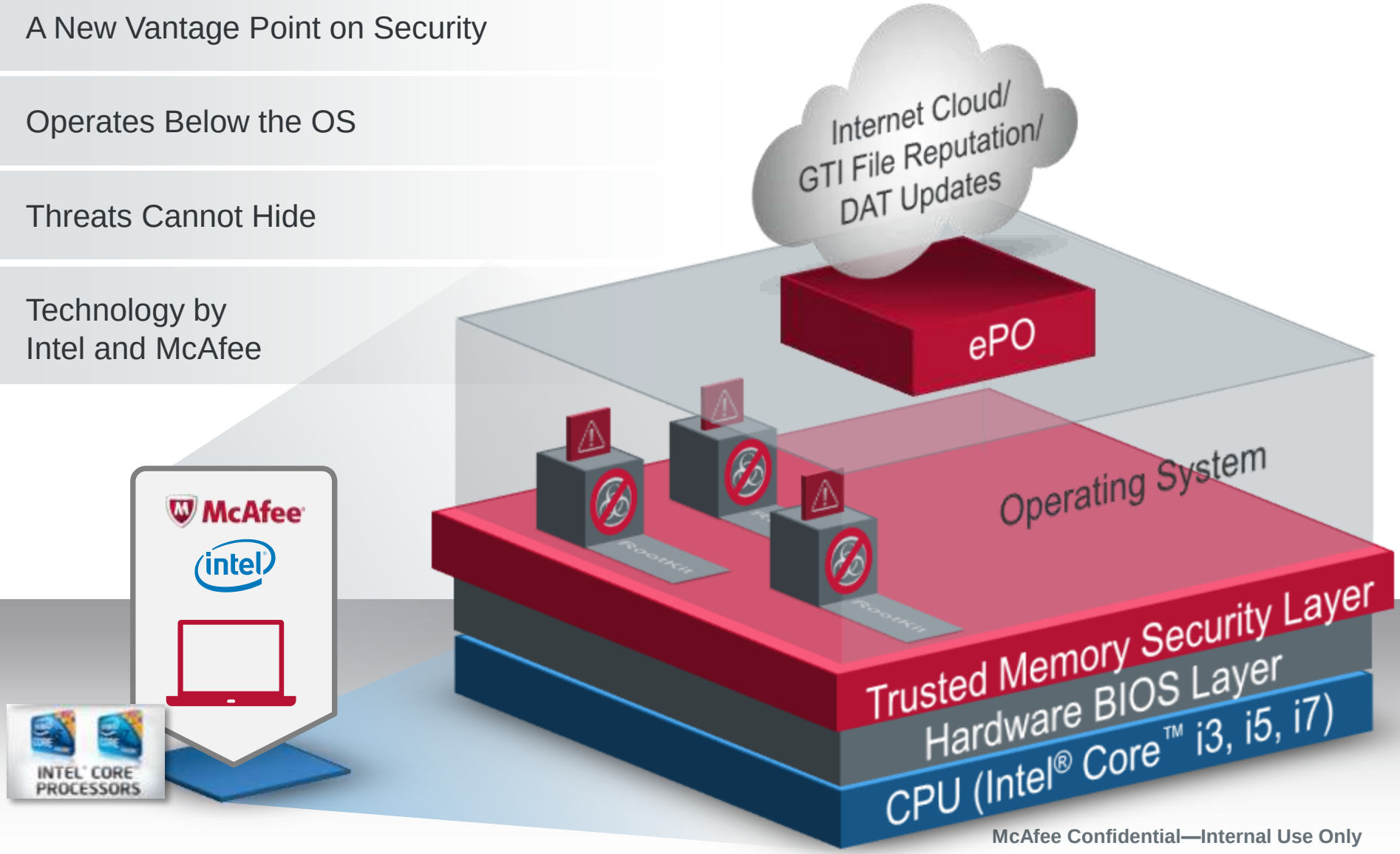
- Operates Within OS
- Will Not Detect Stealth Techniques
- Detection Rates Continue to Decrease




I am not tense. Just terribly, terribly alert.

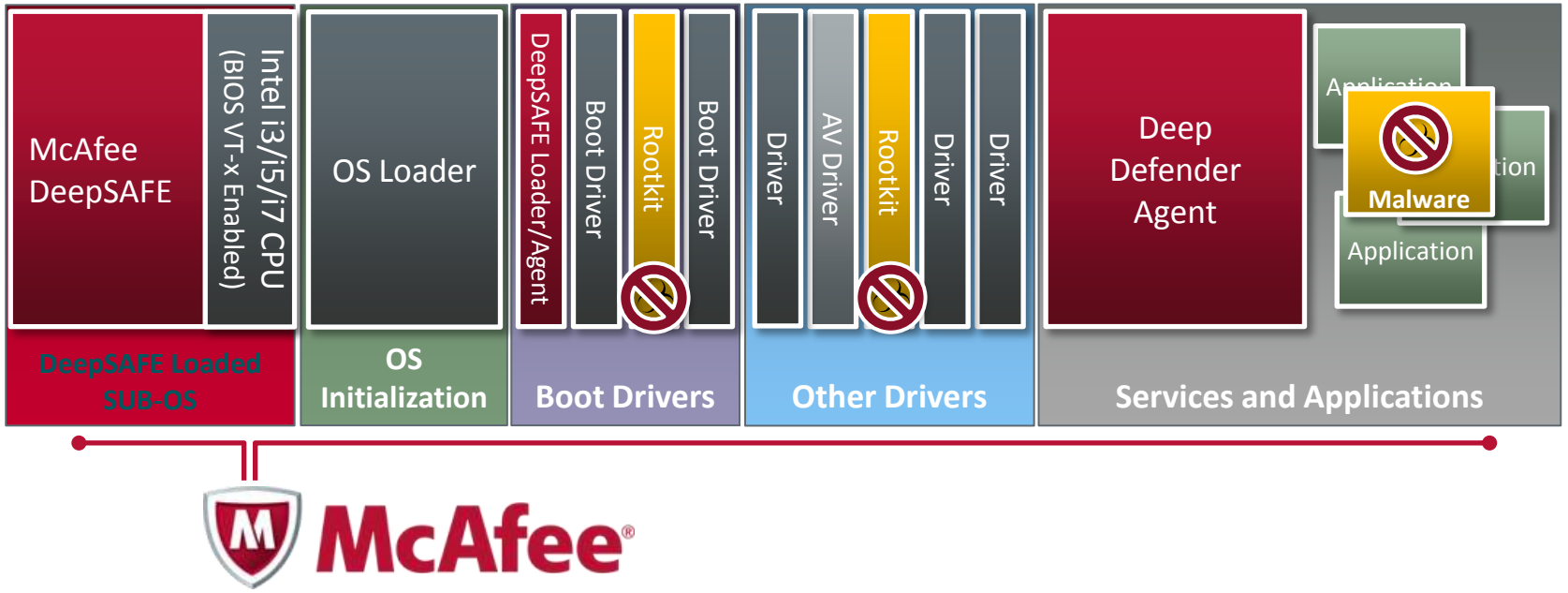
A New Security Platform

- A New Vantage Point on Security
- Operates Below the OS
- Threats Cannot Hide
- Technology by Intel and McAfee



Deep Defender - Stopping a Stealthy Rootkit

- Cooperative Technology – Hardware/Software
- A new vantage point on security
- Operates beneath the OS
- Current threats cannot hide



Sub-OS Security - Customer Benefits

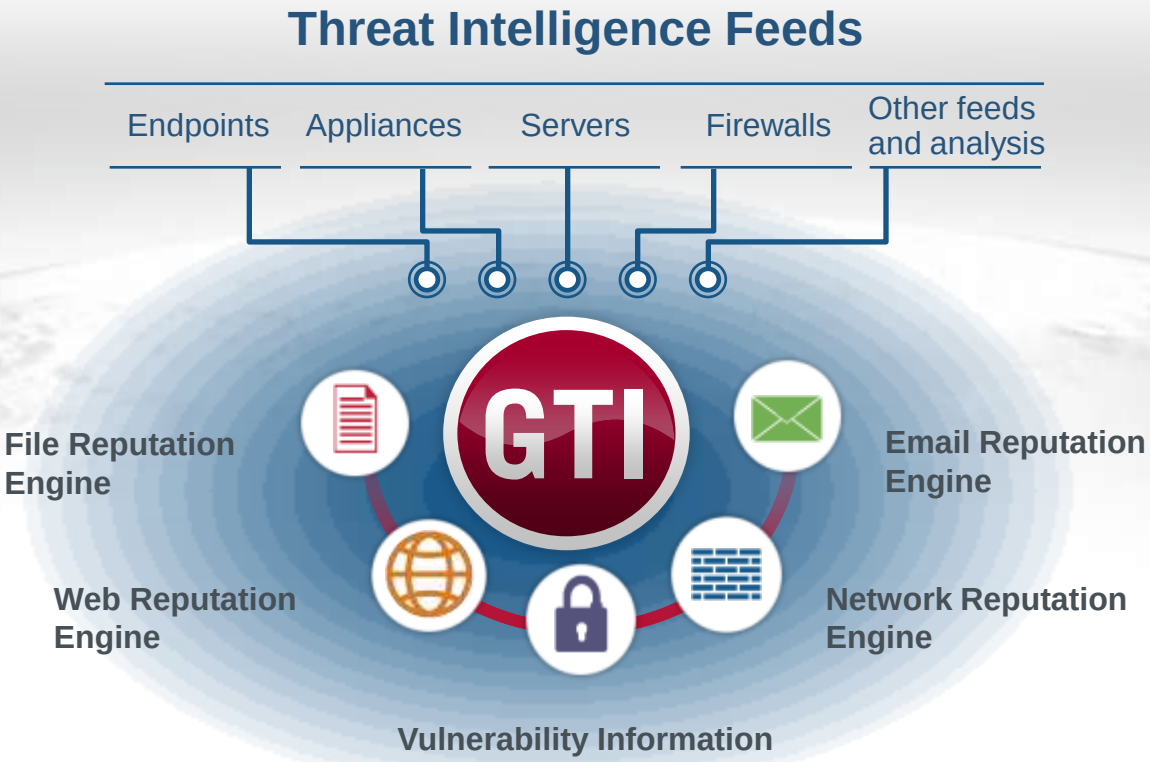
- Expose Hidden Threats
  - Uncover threats you could not see with existing security solution
- Stop Data Loss
  - Prevent the spread of malware designed to steal data that compromise your business
- New Vantage Point on Security
  - Operates beyond the operating systems to detect unknown threats
- Lower Costs
  - Reduce downtime and costs related threat outbreaks

Uncovering The Unknown = Reduced Costs

- Lower number of malware outbreaks
- Cost of single malware outbreak
  - Lost in employee productivity
  - IT administration cost of clean up
  - Remediation costs
- Worldwide cost of malware
  - 13 billion[1]
- Cost per incident
  - Approximate cost per endpoint = $585[2]
  - 5000 node company; 10% infection rate = ~$300k in costs

[1]2007 Computer Economics survey
[2] Estimated 5 hours of IT admin work & 5 hours of loss of employee productivity

Deep Safe Makes Threat Intelligence More Effective



A Few More Details

- Supported current Intel® Core™ i3, i5, i7 processors
- Supports Windows 32 and 64-Bit
- Integrates w/ Cloud Threat Technology - GTI cloud etc.
- Uses Trusted Memory Security Layer (TMSL)
- Open to any and all participants
- A new way of fighting for the Digital Ecosystem
- THE NEW WAY ALSO REQUIRES:

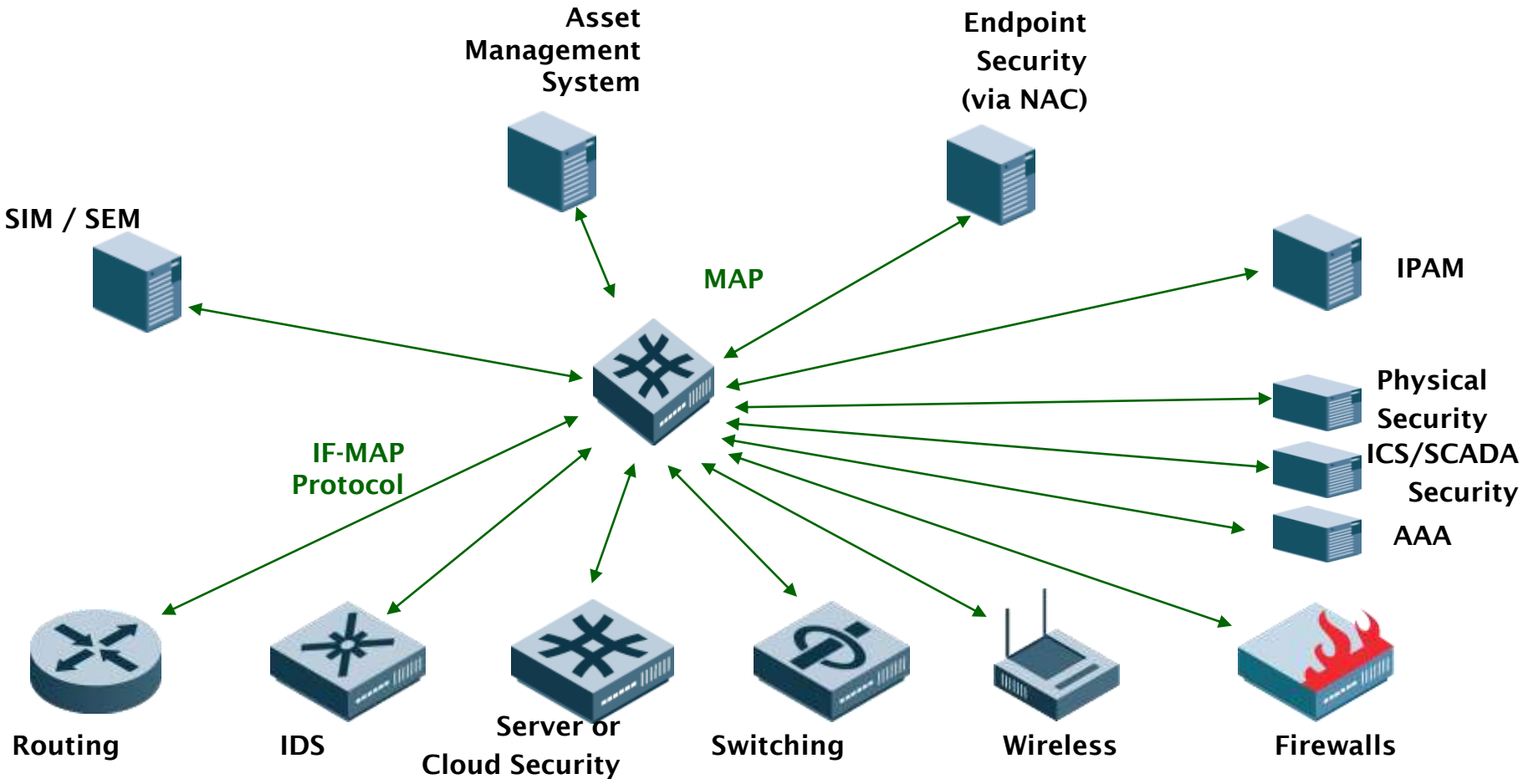
The New Way Requires:

The Community and Industry

To Collaborate

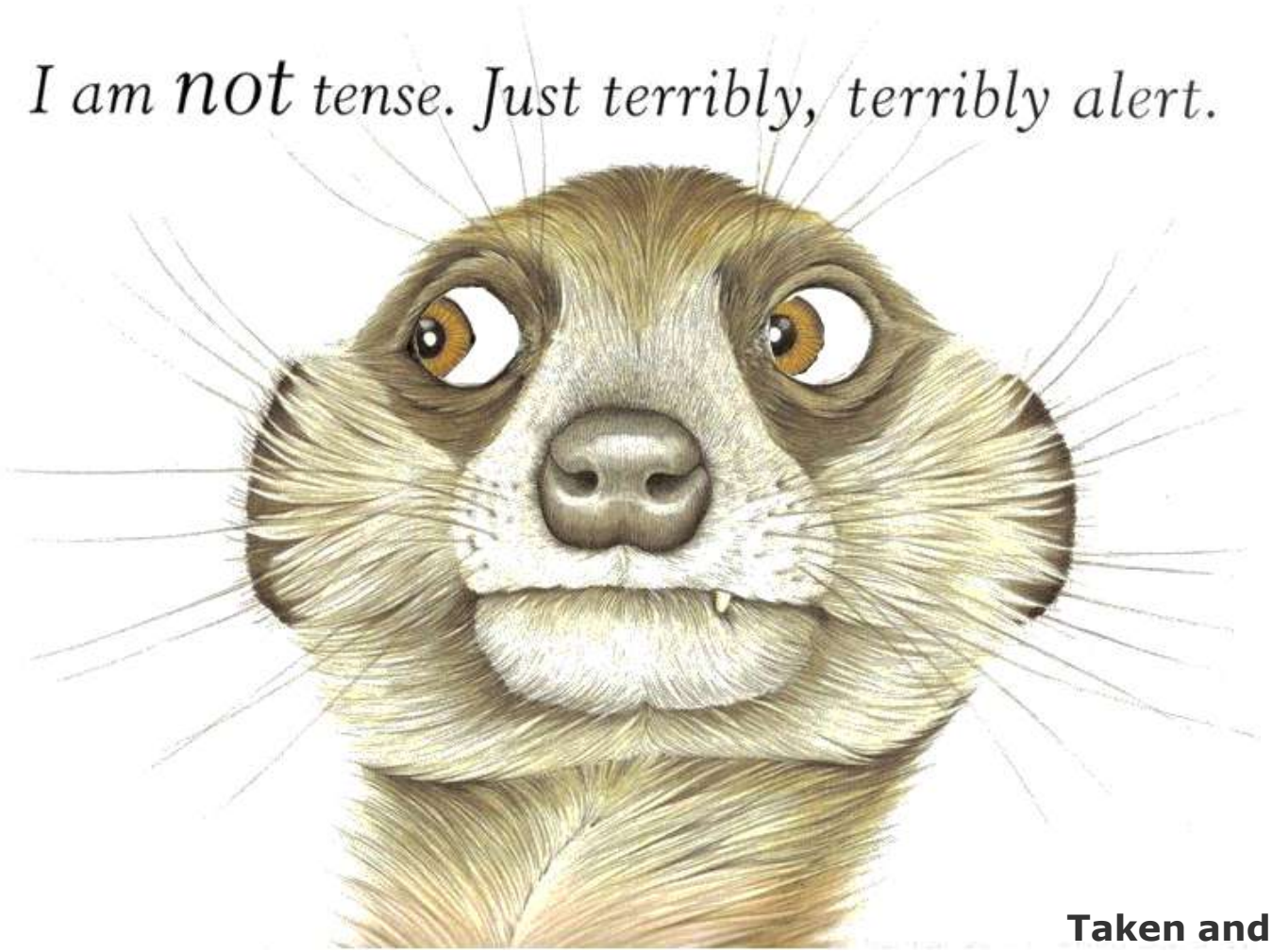
To Conquer

Moving Towards Automated Security



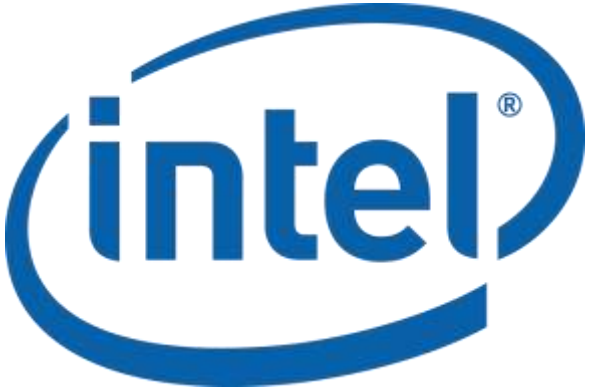
"Recap and Refocus"

- Radical Consumerization Requires More Devices Therefore More Effort
- Nothing Is Getting Easier – Work Smarter
- EndPoints And FlowPoints Are Unmanageable With Any Technology That Will Not Scale From A Visibility Perspective
- Commoditize Where/What You Can
- Innovate Everywhere Else
- **BOTH** Modularity And Scalability Of **Both** Product And Aggregator Of **Relevant Data** Required
- Slow Adoption Of Open Standards and APIs Cripples Innovation Impacting Efficiency And Overall Digital Ecosystem Safety
- We Are All Part Of One Organism In This Digital Ecosystem
- Immune System Concept Holds For Extremities
- "Digital Feudalism" or "Castle And Moat" Were Reasonable In The Past
- Now The "Barbarians" Can Draft Your Citizens, Dogs, Cats, Livestock, Refrigerators, etc. Into Service Against You
- Bad Security Threatens Consumerization Which In Turn Threatens Productivity
- Don't Give Anyone An Excuse



Taken and Modified from Jane Seabrook's 'Furry Logic'

Thank You



Notices

Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

***Other names and brands may be claimed as the property of others.**

**** Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. All dates and product descriptions provided are subject to change without notice. This slide may contain certain forward-looking statements that are subject to known and unknown risks and uncertainties that could cause actual results to differ materially from those expressed or implied by such statements**

*****The threats and attack examples provided in this presentation are intended as examples only. They are not functional and cannot be used to create security attacks. They are not be replicated and/or modified for use in any illegal or malicious activity.**

******Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.**