Intel IT Center

Preventing Stealthy Threats: A Proactive approach from Intel and McAfee

Speakers

John Skinner, Director of Secure Enterprise and Cloud, Intel

Ed Metcalf, Director of Product Marketing for Intel solutions, McAfee

intel

Today's Discussion

Intel IT Center

- The Evolving Threat Landscape
- Computing Trends, Security Implications
- Why a New Approach is Required
- Hardware-Assisted Security Technology
- McAfee Deep Defender
- McAfee Deep Command
- Q & A

Today's Threat Landscape: Hacker *Motivations* Have Expanded....

Intel IT Center

SLAMMER

Hacking for Fun

ZEUS

Organized Crime

AURORA

State-Sponsored Cyber Espionage

STUXNET

Physical Harm

Hacking Software Tools for Sale:
$11B/year industry with 56% CAGR

Industry Problems

Intel IT Center

- 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

intel

Tools of the Modern Hacker

Intel IT Center

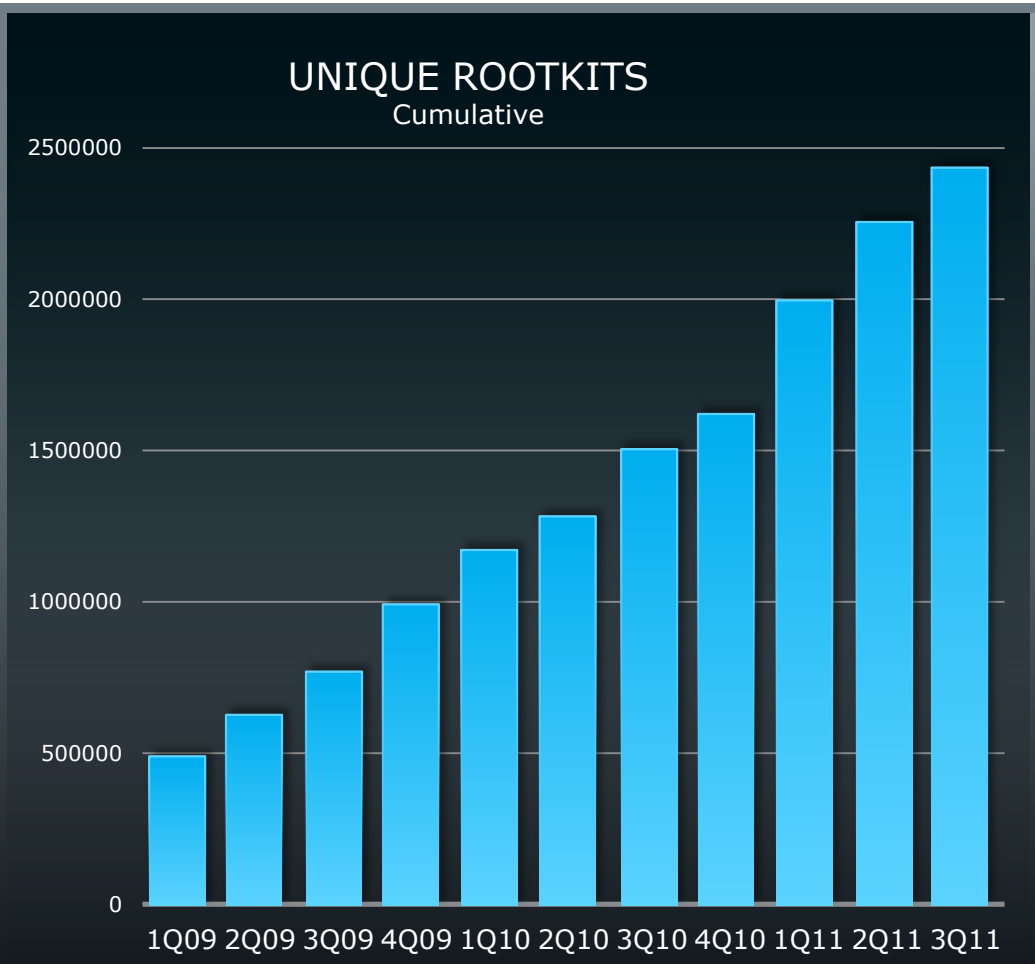
- **Advanced Persistent Threat (APT):**

  A long term, human-directed "campaign" to take control of a specific system or network – all while remaining undetected.

- **Kernel-mode Rootkit:**

  Lives and operates below the operating system, and evades detection by OS-level security measures. Cloaks other malware & APT's.

Stealth Malware Explosion



- Stealth techniques drive proliferation of malware
- Designed to evade traditional security measures
- Cyber criminals using more stealth to hide data-stealing malware
  - 110,000 new rootkits each quarter
  - 1,200 new rootkits per day
- More malware using rootkits to evade detection
  - Stuxnet
  - Koobface
  - SpyEye
  - TDSS

Stealth Techniques Increases Risk Exposure

Intel IT Center

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

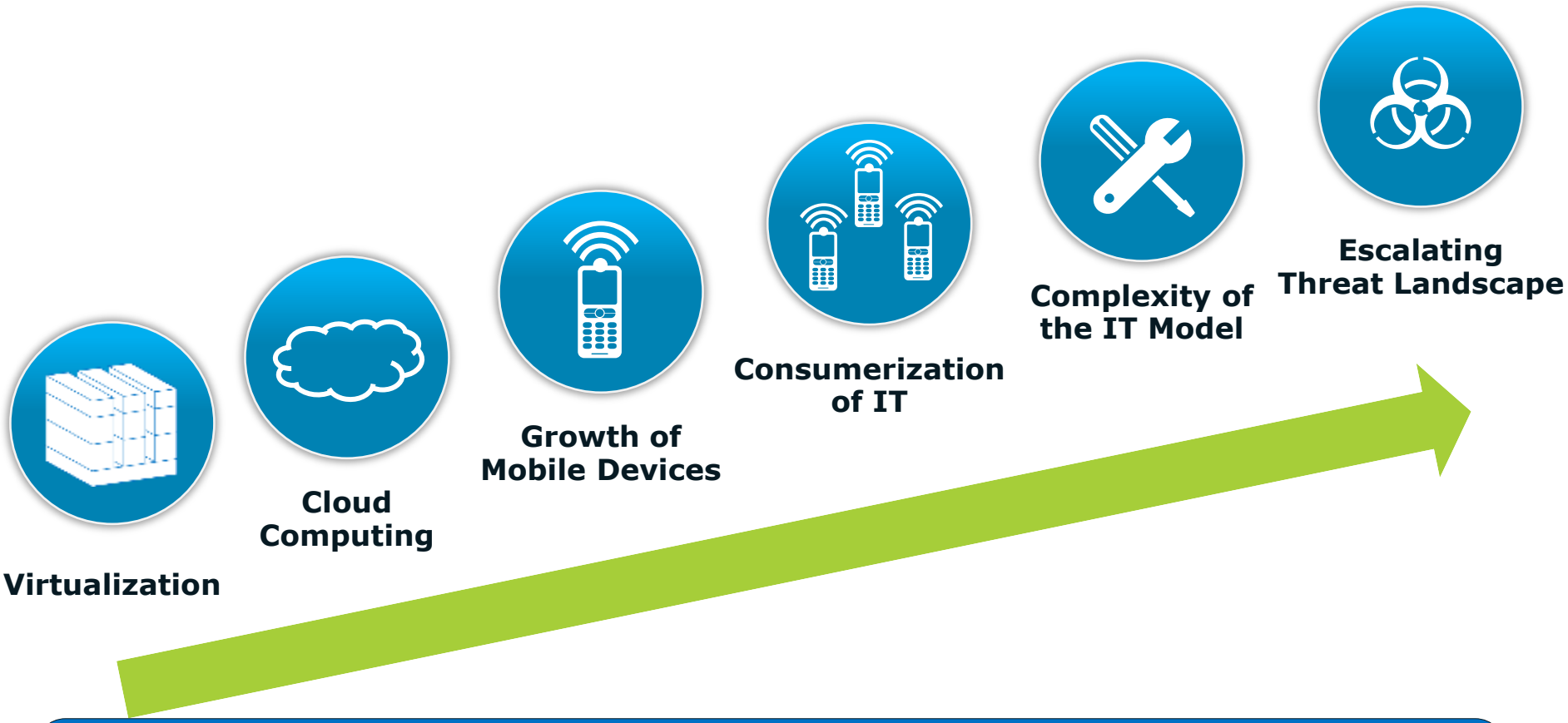
Koobface threat used stealth techniques to secretly turn an endpoint into a BOT

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

Computing Trends and Security Implications

Intel IT Center



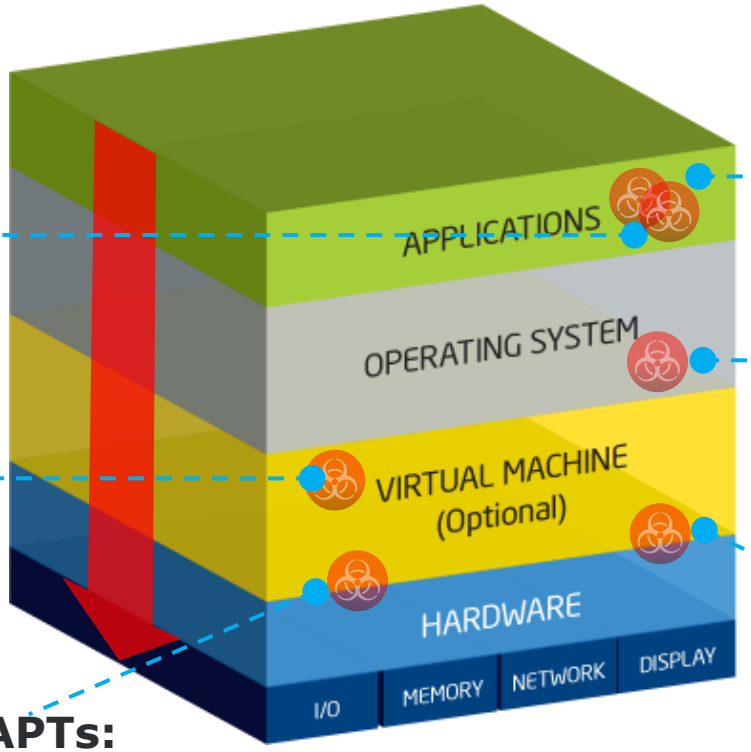
As a consequence:
the size of the "Attack Surface" and the opportunities for Malicious Entry have expanded.

Attacks Are Moving "Down the Stack", to Gain Greater Stealth and System Control

Intel IT Center

Attacks disable security products

Compromise virtual machine



Traditional attacks: Focused primarily on the application layer

OS infected with APTs: Threats are hidden from security products

Ultimate APTs: Compromise platform and devices below the OS, using rootkits as cloaks

New stealth attacks: Embed themselves below the OS and Virtual Machine, so they can evade current solutions

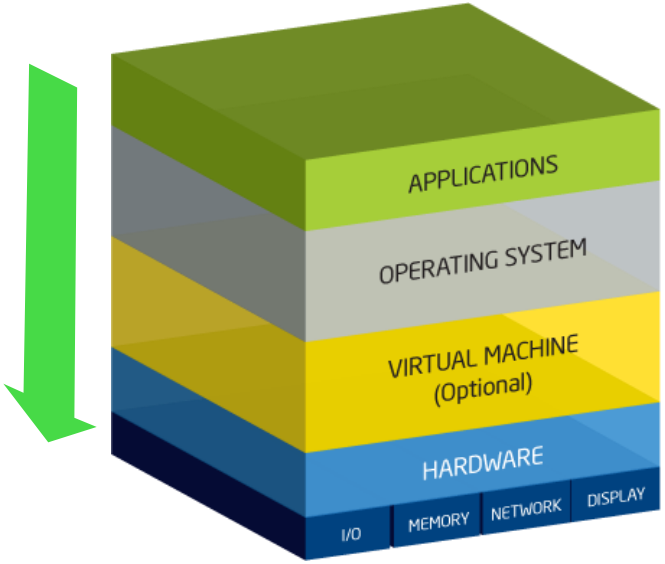
APT: Advanced Persistent Threat

intel

A New Approach Is Required:
"Hardware-assisted Security"

Intel IT Center

- **Move critical security processes *down into the hardware***
  - Encryption, Authentication, Manageability, and Platform Cleansing
  - Hardware is inherently less vulnerable to modification or corruption
- Establish **a security perimeter from the hardware layer up**
- **Isolate** the security services from the host OS (often the target)
- Build in capability to **monitor, maintain, repair, and recover**

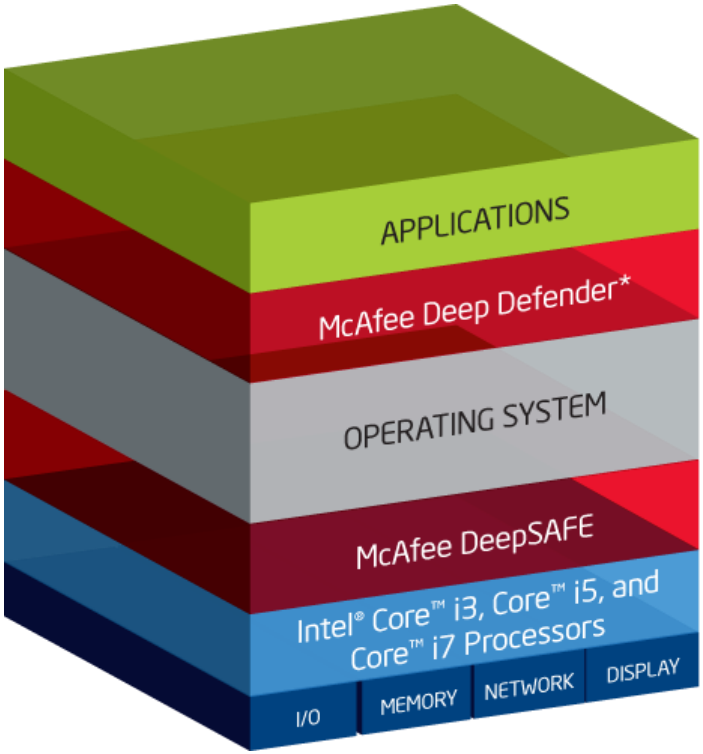


Added Protection against:

- Viruses and worms
- Malware
- Disabled software
- ***Rootkits***

Example of Hardware-assisted Security: McAfee DeepSAFE Security Platform

Intel IT Center



- **DeepSAFE is the first hardware-assisted security platform from Intel and McAfee, utilizing Intel Virtualization Technology. Platform capabilities include:**
  - McAfee Deep Defender* product
    - Utilizes the isolation capabilities of Intel Virtualization Technology
    - Works "beyond" the OS, so it can't be corrupted by OS or malware
    - Detects, blocks, and removes stealthy advanced persistent threats and malware
  - Foundation for future solutions from McAfee and Intel

Next-generation "beyond the OS" security enabled by Intel® processor technology

intel

Deep Defender—Stopping a Stealthy Rootkit

Intel IT Center

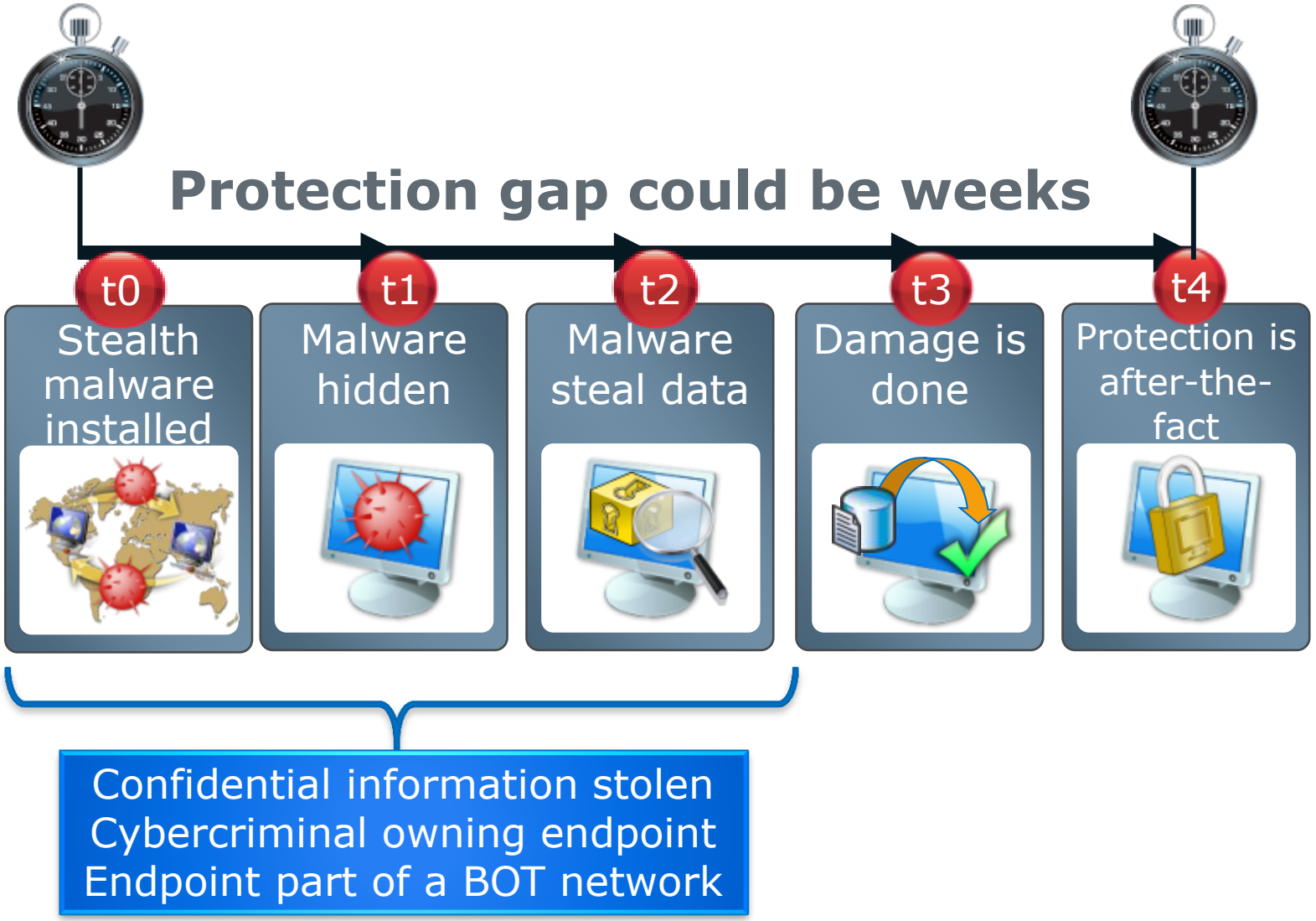
McAfee

- Real-time kernel-level monitor of memory
- Identifies kernel-mode rootkits in real-time
- Prevents the drivers from loading
- DeepSAFE technology loads before the OS
- DeepSAFE technology informs Deep Defender of suspicious behavior

intel

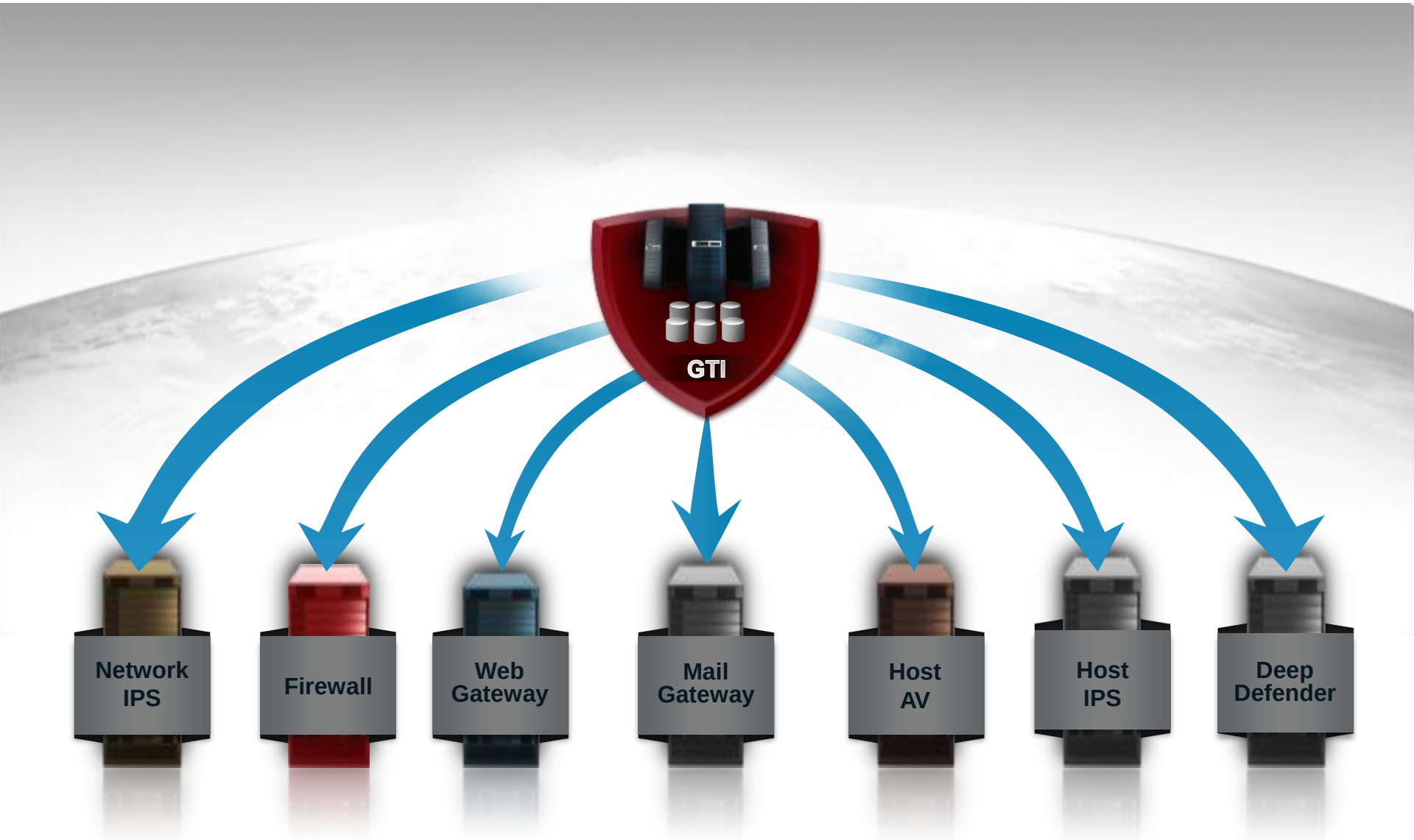
Stealth Rootkits – After the Fact is Too Late!

Intel IT Center



Deep Defender Enabling Global Threat Intelligence

Intel IT Center



Deep Defender Deployment Details

Intel IT Center

- Supported Intel chipsets
  - Intel® Core™ i3, i5, i7 processors
- Supports Windows 7; 32 & 64 bit
- Integrates with McAfee's GTI cloud
- Utilizes Intel VT in the Core iSeries processors

intel

Talk to an Expert: Question & Answer

Intel IT Center

Today's experts:

John Skinner, Director of Secure Enterprise and Cloud, Intel

Ed Metcalf, Director of Product Marketing for Intel solutions, McAfee

Submit your questions:

- Ask questions at anytime by pressing the Question tab at the top of the player.

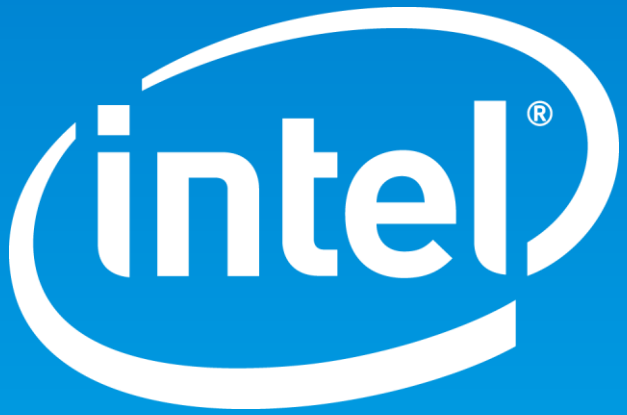
More information:

- Download content at the top of the player
- Visit www.intel.com/pcsecurity
- Check out the Intel IT Center, a valuable source of unbiased, relevant information to help you meet your most challenging IT demands: www.intel.com/itcenter

Legal Notices and Disclaimers

Intel IT Center

intel


intel